

# GENERALIZED MORDELL CURVES, GENERALIZED FERMAT CURVES, AND THE HASSE PRINCIPLE

NGUYEN NGOC DONG QUAN

## CONTENTS

1. Introduction	1
2. Non-existence of rational points on certain generalized Mordell curves	5
3. A subset of the set of all rational points on $\mathcal{X}_p$	10
4. Certain generalized Mordell curves violating the Hasse principle	13
4.1. A sufficient condition	13
4.2. Infinitude of the triples $(p, n, \kappa)$	15
5. The descending chain condition on sequences of curves	18
6. Certain generalized Fermat curves violating the Hasse principle	22
7. Infinitude of the quadruples $(p, n, \kappa, \chi)$	25
8. The descending chain condition on sequences of generalized Fermat curves	32
9. Epilogue	35
Acknowledgements	45
References	45

**ABSTRACT.** A generalized Mordell curve of degree  $n \geq 3$  over  $\mathbb{Q}$  is the smooth projective model of the affine curve of the form  $Az^2 = Bx^n + C$ , where  $A, B, C$  are nonzero integers. A generalized Fermat curve of signature  $(n, n, n)$  with  $n \geq 3$  over  $\mathbb{Q}$  is the smooth projective curve of the form  $Ax^n + By^n + Cz^n = 0$  for some nonzero integers  $A, B, C$ . In this paper, we show that for each prime  $p$  with  $p \equiv 1 \pmod{8}$  and  $p \equiv 2 \pmod{3}$ , there exists a threefold  $\mathcal{X}_p \subseteq \mathbb{P}^6$  such that certain rational points on  $\mathcal{X}_p$  produce infinite families of non-isomorphic generalized Mordell curves of degree  $12n$  and infinite families of generalized Fermat curves of signature  $(12n, 12n, 12n)$  for each  $n \geq 2$  that are counterexamples to the Hasse principle explained by the Brauer-Manin obstruction. We also show that the set of special rational points on  $\mathcal{X}_p$  producing generalized Mordell curves and generalized Fermat curves that are counterexamples to the Hasse principle is infinite, and can be constructed explicitly.

## 1. INTRODUCTION

Faltings' theorem, née the Mordell conjecture states that a smooth geometrically irreducible curve over a number field has only finitely many rational points. Despite of this celebrated result, the following open problem remains widely open: For a family of smooth geometrically irreducible curves  $\mathcal{C}$  over a number field  $\mathbb{Q}$ , determine the sets  $\mathcal{C}(\mathbb{Q})$  of all rational points on the curves  $\mathcal{C}$ . This problem remains open even in the case where we assume further that the family of curves  $\mathcal{C}$  under consideration only consists of *generalized Mordell curves* and *generalized Fermat curves*.

For a positive integer  $n \geq 3$ , a *generalized Mordell curve of degree  $n$*  over  $\mathbb{Q}$  is the smooth projective model of the affine curve defined by

$$Az^2 = Bx^n + C,$$

---

*Date:* December 12, 2012.

*2010 Mathematics Subject Classification.* Primary 14G05, 11G35, 11G30.

*Key words and phrases.* Azumaya algebras, Brauer groups, Brauer-Manin obstruction, Hasse principle, generalized Mordell curves, generalized Fermat curves.

where  $A, B, C$  are nonzero integers. Although the defining equations of generalized Mordell curves are simple-looking, the problem of finding all rational points on the family of all generalized Mordell curve of arbitrary degree remains widely open. There are several authors studying the arithmetic of generalized Mordell curves. In 2004, Bennett and Skinner [1] developed techniques for finding all rational points on certain generalized Mordell curves of the form  $Az^2 = Bx^n + C$  for certain choices of integers  $A, B, C$ . Their techniques rely on the theory of elliptic curves, Galois representations, and modular forms, and was previously used by Wiles in his celebrated proof of Fermat's last theorem (see [14]). In [5], Ivorra and Kraus studied the arithmetic of certain generalized Mordell curves of the shape  $Az^2 = Bx^p + C$ , where  $p$  is an odd prime.

For a positive integer  $n \geq 3$ , a *generalized Fermat curve of signature  $(n, n, n)$*  over  $\mathbb{Q}$  is the projective curve defined by

$$Ax^n + By^n + Cz^n = 0,$$

where  $A, B, C$  are nonzero integers such that  $\gcd(A, B, C) = 1$ . There are several authors studying the arithmetic of generalized Fermat curves; for example, Selmer [12] constructed the generalized Fermat curve of signature  $(3, 3, 3)$  defined by

$$3x^3 + 4y^3 + 5z^3 = 0,$$

which is the first cubic curve of genus one violating the Hasse principle. In [14], Wiles proved Fermat's last theorem, which says that the only rational points on the Fermat curve  $x^n + y^n = z^n$  with  $n \geq 3$  are the trivial ones.

In this paper, we are concerned with studying nonexistence of rational points on certain families of generalized Mordell curves of degree  $12n$  with  $n \geq 1$  and of generalized Fermat curves of signature  $(12n, 12n, 12n)$  with  $n \geq 1$ . The basic technique used in this paper is the Brauer-Manin obstruction. It is also crucial that we need to obtain information about rational points on certain higher dimensional varieties to determine the arithmetic of certain families of curves that we consider throughout this work. To add interest to the arithmetic of these curves, we require that they have points over each local field  $\mathbb{Q}_p$  for each prime  $p$  including  $p = \infty$ , and hence these families of curves are counterexamples to the *Hasse principle*.

Let us digress for a moment to review some basic notions in the Brauer-Manin obstruction. Recall that the *Hasse reciprocity law* (see [13]) states that the sequence of abelian groups

$$0 \rightarrow \mathrm{Br}(\mathbb{Q}) \rightarrow \bigoplus_p \mathrm{Br}(\mathbb{Q}_p) \rightarrow \mathbb{Q}/\mathbb{Z} \rightarrow 0$$

is exact, where for each scheme  $\mathcal{X}$ , we denote by  $\mathrm{Br}(\mathcal{X})$  the Brauer group of  $\mathcal{X}$  and for a commutative ring  $A$ , define

$$\mathrm{Br}(A) := \mathrm{Br}(\mathrm{Spec}(A)).$$

In 1970, Manin [7], based on the Hasse reciprocity law, introduced the notion of the Brauer-Manin obstruction. Roughly speaking, the Brauer-Manin obstruction measures how badly the Hasse principle for varieties fails.

Take a smooth geometrically irreducible curve  $\mathcal{C}$  defined over  $\mathbb{Q}$ , and let  $\mathbb{A}_{\mathbb{Q}}$  be the ring of rational adeles. Let  $\mathcal{C}(\mathbb{A}_{\mathbb{Q}})$  denote the set of adelic points on  $\mathcal{C}$ . It is well-known that

$$\mathcal{C}(\mathbb{A}_{\mathbb{Q}}) = \prod_p \mathcal{C}(\mathbb{Q}_p).$$

Manin [7] introduced a subset of  $\mathcal{C}(\mathbb{A}_{\mathbb{Q}})$ , say  $\mathcal{C}(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}}$ , such that

$$\mathcal{C}(\mathbb{Q}) \subseteq \mathcal{C}(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}} \subseteq \mathcal{C}(\mathbb{A}_{\mathbb{Q}}).$$

Here  $\mathcal{C}(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}}$  is defined to be the right kernel of the *adelic Brauer-Manin pairing* (see [13])

$$(1) \quad \begin{aligned} \mathcal{E} : \mathrm{Br}(\mathcal{C}) \times \mathcal{C}(\mathbb{A}_{\mathbb{Q}}) &\longrightarrow \mathbb{Q}/\mathbb{Z} \\ (\mathcal{A}, (P_p)_p) &\mapsto \sum_p \mathrm{inv}_p(\mathcal{A}(P_p)), \end{aligned}$$

where for each prime  $p$ ,  $\text{inv}_p : \text{Br}(\mathbb{Q}_p) \rightarrow \mathbb{Q}/\mathbb{Z}$  is the invariant map of local class field theory. We say that  $\mathcal{C}$  *satisfies the Hasse principle* if the following holds:  $\mathcal{C}(\mathbb{Q}) \neq \emptyset$  if and only if  $\mathcal{C}(\mathbb{A}_{\mathbb{Q}}) \neq \emptyset$ . We say that  $\mathcal{C}$  is a *counterexample to the Hasse principle* if  $\mathcal{C}(\mathbb{Q}) = \emptyset$  but  $\mathcal{C}(\mathbb{A}_{\mathbb{Q}}) \neq \emptyset$ . Furthermore, we say that  $\mathcal{C}$  is a *counterexample to the Hasse principle explained by the Brauer-Manin obstruction* if  $\mathcal{C}$  is a counterexample to the Hasse principle and satisfies  $\mathcal{C}(\mathbb{A}_{\mathbb{Q}})^{\text{Br}} = \emptyset$ .

Let  $p$  be a prime such that  $p \equiv 1 \pmod{8}$ . Here, as throughout this paper, we denote by  $\mathcal{X}_p$  the threefold in  $\mathbb{P}_{\mathbb{Q}}^6$  defined by

$$(2) \quad \mathcal{X}_p : \begin{cases} b^2 - c^2 + 2pef &= 0 \\ 2ab - 2cd + pf^2 &= 0 \\ a^2 - d^2 + pg^2 &= 0 \end{cases}$$

We now introduce certain rational points on  $\mathcal{X}_p$  which are of great interest throughout this paper.

**Definition 1.1.** Let  $p$  be a prime such that  $p \equiv 1 \pmod{8}$ . Let  $n$  be a positive integer such that  $n \geq 1$ . Let  $(A, B, C, D, E, F, G) \in \mathbb{Z}^7$  be a septuple of integers such that at least one of them is non-zero. We say that  $(A, B, C, D, E, F, G)$  *satisfies Hypothesis FM with respect to the couple  $(p, n)$*  if the following are true:

- (A1) the point  $\mathcal{P} := (a : b : c : d : e : f : g) = (A : B : C : D : E : F : G)$  belongs to  $\mathcal{X}_p(\mathbb{Q})$ .
- (A2) let  $l$  be any odd prime such that  $\gcd(l, 3) = \gcd(l, p) = 1$  and  $l$  divides  $E$ . Then  $p$  is a square in  $\mathbb{Q}_l^{\times}$  or  $v_l(E) - v_l(G) < 6n$ .
- (A3)  $\gcd(A, D, G) = 1$ ,  $E \not\equiv 0 \pmod{p}$  and  $G \not\equiv 0 \pmod{p}$ .
- (A4) let  $l$  be any odd prime such that  $\gcd(l, 3) = \gcd(l, p) = 1$  and

$$\gcd(AC - BD, DE - CF, AE - BF) \equiv 0 \pmod{l}.$$

Then  $p$  is a square in  $\mathbb{Q}_l^{\times}$ .

- (A5) there exists an integer  $H$  such that  $G - EH^6 \equiv 0 \pmod{p}$  and  $A + \zeta BH^4$  is a quadratic non-residue in  $\mathbb{F}_p^{\times}$  for any cube root of unity  $\zeta$  in  $\mathbb{F}_p^{\times}$ .

Moreover, if 3 is a quadratic non-residue in  $\mathbb{F}_p^{\times}$ , we further assume that the following are true:

- (A6)  $v_3(E) - v_3(G) < 6n$
- (A7)  $A + B \not\equiv 0 \pmod{3}$  and  $G \equiv 0 \pmod{3}$ .

**Remark 1.2.** Since  $p \equiv 1 \pmod{8}$ , it follows from the quadratic reciprocity law that  $-3$  is not a square in  $\mathbb{F}_p^{\times}$  if and only if  $p$  is not a square in  $\mathbb{F}_3^{\times}$ , or equivalently  $p \equiv 2 \pmod{3}$ . Hence if  $p \equiv 2 \pmod{3}$ , then the group of all cube roots of unity in  $\mathbb{F}_p^{\times}$  is trivial. Thus (A5) is tantamount to the condition that there exists an integer  $H$  such that  $G - EH^6 \equiv 0 \pmod{p}$  and  $A + BH^4$  is a quadratic non-residue in  $\mathbb{F}_p^{\times}$ .

**Remark 1.3.** Note that Hypothesis FM implies that  $A, D, E$  and  $G$  are nonzero. Indeed, by (A3), we know that  $E, G \not\equiv 0 \pmod{p}$ , and hence  $E, G$  are nonzero. Assume that  $A = 0$ . Then, by (A1) and the third equation of (2), we see that  $D^2 = pG^2$ . Hence  $p = \left(\frac{D}{G}\right)^2$ , which is a contradiction since  $p$  is a prime. Hence  $A \neq 0$ . Assume that  $D = 0$ . Then, by (A1) and the third equation of (2), we deduce that  $A^2 + pG^2 = 0$ , which is a contradiction since  $A^2 + pG^2 > 0$ . Hence  $D \neq 0$ .

For a prime  $p \equiv 1 \pmod{8}$ , a positive integer  $n$ , and each septuple  $(A, B, C, D, E, F, G)$  satisfying Hypothesis FM with respect to  $(p, n)$ , we will produce an Azumaya algebra  $\mathcal{A}$  on the generalized Mordell curve  $\mathcal{C}$  of the shape  $pz^2 = E^2x^{12n} - G^2$ . The construction of the Azumaya algebra  $\mathcal{A}$  relies mainly on the equations of the threefold  $\mathcal{X}_p$ . Using conditions (A1) – (A7), we will show that  $\mathcal{A}$  satisfies

$$\text{inv}_l(\mathcal{A}(P_l)) = \begin{cases} 0 & \text{if } l \neq p, \\ 1/2 & \text{if } l = p \end{cases}$$

for any  $P_l \in \mathcal{C}(\mathbb{Q}_l)$ . From these invariants of the Azumaya algebra  $\mathcal{A}$ , it follows that  $\mathcal{C}(\mathbb{A}_{\mathbb{Q}})^{\text{Br}} = \emptyset$ , and thus the generalized Mordell curve  $\mathcal{C}$  of degree  $12n$  has no rational points. More precisely, we will prove the following.

**Theorem 1.4.** (see Theorem 2.2)

Let  $p$  be a prime such that  $p \equiv 1 \pmod{8}$ , and let  $n$  be a positive integer. Let  $(A, B, C, D, E, F, G)$  be a septuple of integers satisfying Hypothesis FM with respect to  $(p, n)$ . Then the generalized Mordell curve  $\mathcal{C}$  defined by

$$\mathcal{C} : pz^2 = E^2 x^{12n} - G^2$$

satisfies  $\mathcal{C}(\mathbb{A}_{\mathbb{Q}})^{\text{Br}} = \emptyset$ .

The basic technique that we exploit in the proof of Theorem 1.4 is based upon the Brauer-Manin obstruction, and thus our method of studying the arithmetic of generalized Mordell curves is completely different from that appeared in [1] and [5] in which the authors mainly used the modularity method. Moreover, in order to use the Brauer-Manin obstruction to show that certain generalized Mordell curves possess no rational points, it is crucial that we need to obtain information about the set of rational points on  $\mathcal{X}_p$  satisfying Hypothesis FM. The existence of rational points on the threefolds  $\mathcal{X}_p$  satisfying Hypothesis FM that proves nonexistence of rational points on certain generalized Mordell curves suggests that there exist certain higher dimensional varieties which play an important role in studying the arithmetic of certain curves. In this work, we introduce threefolds  $\mathcal{X}_p$  for each prime  $p \equiv 1 \pmod{8}$ , and show that the existence of a subset of  $\mathcal{X}_p(\mathbb{Q})$  consisting of rational points on  $\mathcal{X}_p$  that satisfy Hypothesis FM is equivalent to the existence of certain families of generalized Mordell curves and of generalized Fermat curves having no rational points. Thus the arithmetic of threefolds  $\mathcal{X}_p$  determine the arithmetic of a special class of curves including certain generalized Mordell curves and certain generalized Fermat curves.

Let  $p$  be a prime such that  $p \equiv 1 \pmod{8}$  and  $p \equiv 2 \pmod{3}$ , and let  $n$  be a positive integer such that  $n \geq 2$ . In Section 3, we will describe an infinite subset of  $\mathcal{X}_p(\mathbb{Q})$  that consists of rational points on  $\mathcal{X}_p$  satisfying Hypothesis FM with respect to  $(p, n)$ . This subset is parameterized by three parameters  $\alpha, \beta, \kappa$ . For some choice of  $\kappa$ , and by Theorem 1.4, we prove that there exist infinitely many non-isomorphic generalized Mordell curves of the shape  $pz^2 = 3^6 \kappa^6 x^{12n} - 1$  that are counterexamples to the Hasse principle explained by the Brauer-Manin obstruction. This result is the combination of Theorem 4.2 and Corollary 4.4.

For any positive integer  $m$  such that  $2m < n$ , we will show that there are infinitely many integers  $\kappa$  such that the generalized Mordell curve  $\mathcal{D}_{(p,m)}^{(\kappa)}$  has at least two rational points in its affine locus whereas the generalized Mordell curve  $\mathcal{D}_{(p,n)}^{(\kappa)}$  is a counterexample to the Hasse principle explained by the Brauer-Manin obstruction, where  $\mathcal{D}_{(p,m)}^{(\kappa)}$  and  $\mathcal{D}_{(p,n)}^{(\kappa)}$  are defined by

$$\mathcal{D}_{(p,m)}^{(\kappa)} : pz^2 = 3^6 \kappa^6 x^{12m} - 1$$

and

$$\mathcal{D}_{(p,n)}^{(\kappa)} : pz^2 = 3^6 \kappa^6 x^{12n} - 1,$$

respectively. This is Lemma 5.3 in Section 5. This result also shows that the degree  $12n$  of the generalized Mordell curves in Theorem 1.4 is *optimal* in the sense that one can not replace  $n$  by any positive divisor  $s$  of  $n$  with  $s \neq n$ . This will be explained in more detail in Remark 5.4.

In Section 5, motivated by Lemma 5.3, we introduce a notion of the *descending chain condition* (DCC) on sequences of curves, which is an analogue of the notion of the descending chain condition on partially ordered sets. Let  $(\mathcal{X}_n, \psi_n)_{n \geq 1}$  be a sequence of curves defined over a global field  $k$ , where for each  $n \geq 1$ ,  $\mathcal{X}_n$  is a curve of genus  $g_n$  defined over  $k$ , and for each  $n \geq 1$ ,  $\psi_n : \mathcal{X}_{n+1} \rightarrow \mathcal{X}_n$  is a  $k$ -morphism of curves. The sequence  $(\mathcal{X}_n, \psi_n)_{n \geq 1}$  is said to satisfy the DCC of length  $h$  if  $\mathcal{X}_n(k) \neq \emptyset$  for each  $1 \leq n \leq h-1$ , and  $\mathcal{X}_h$  is a counterexample to the Hasse principle explained by the Brauer-Manin obstruction. To rule out certain trivial cases, we assume that  $g_n > g_m$  for any positive integers  $n > m$ . It is not difficult to see that there are infinitely many sequences of curves that do not satisfy the DCC of any length. However, constructing sequences of curves satisfying the DCC of arbitrary length seems a nontrivial problem. In Section 5, we will show that there exist infinitely many sequences of generalized

Mordell curves that satisfy the DCC of arbitrary length, and hence these sequences provide a nontrivial class of sequences of curves satisfying the DCC. This will be proved in Corollary 5.5.

Sections 6 and 7 are motivated by the following problem, which was first studied by Halberstadt and Kraus [4].

**Problem 1.5.** (see [4, Problème 3 and Problème 4])

*For each prime  $p \geq 3$ , does there exist an explicit generalized Fermat curve  $\mathcal{C}$  of signature  $(p, p, p)$  defined over  $\mathbb{Q}$  of the shape  $Ax^p + By^p + Cz^p = 0$  that is a counterexample to the Hasse principle?*

As was mentioned before, Selmer [12] constructed the generalized Mordell curve defined by  $3x^3 + 4y^3 + 5z^3 = 0$  that violates the Hasse principle, and hence Problem 1.5 holds for  $p = 3$ . For each prime  $p$  with  $5 \leq p \leq 100$ , Halberstadt and Kraus [4] constructed an explicit generalized Fermat curve of signature  $(p, p, p)$  that violates the Hasse principle. Hence Problem 1.5 holds for each prime  $p$  between 5 and 100. Furthermore, assuming the abc conjecture, Halberstadt and Kraus [4] proved that Problem 1.5 holds for every prime  $p \geq 5$ .

In Problem 1.5, the reason why we only consider certain generalized Fermat curves of signature  $(p, p, p)$  with  $p$  prime is that we want to rule out certain trivial cases, and that we do not want  $p$  to be replaced by any positive divisor  $s$  of  $p$  with  $s \neq p$ . Motivated by this observation, we generalize Problem 1.5, and study the following problem.

**Problem 1.6.** *For each positive integer  $n \geq 3$ , does there exist an explicit generalized Fermat curve  $\mathcal{C}_n$  of signature  $(n, n, n)$  defined over  $\mathbb{Q}$  of the shape  $Ax^n + By^n + Cz^n = 0$  with  $\gcd(A, B, C) = 1$  that is a counterexample to the Hasse principle explained by the Brauer-Manin obstruction such that for any positive divisor  $s$  of  $n$  with  $s \neq n$ , the generalized Fermat curve  $\mathcal{C}_s$  of signature  $(s, s, s)$  defined by  $Ax^s + By^s + Cz^s = 0$  has at least one rational point?*

Upon assuming that  $n$  is a prime, we see that Problem 1.5 is a special case of Problem 1.6. In Sections 6 and 7, we answer Problem 1.6 in the affirmative for any positive integer  $n \equiv 0 \pmod{12}$  with  $n \geq 24$ . In fact, we prove that for each positive integer  $n \equiv 0 \pmod{12}$  with  $n \neq 12$ , there are infinitely many generalized Fermat curves  $\mathcal{C}_n$  of signature  $(n, n, n)$  satisfying Problem 1.6. This result is the combination of Theorem 6.2 and Lemma 7.5. As a consequence, in Section 8, we show that there exist infinitely many sequences of generalized Fermat curves that satisfy the DCC of any length.

In the last section, we describe another subset of  $\mathcal{X}_p(\mathbb{Q})$ , and prove that upon assuming Schinzel's Hypothesis H (which will be reviewed in the same section), there should exist another infinite subset of  $\mathcal{X}_p(\mathbb{Q})$  consisting of rational points on  $\mathcal{X}_p$  that satisfy Hypothesis FM with respect to  $(p, n)$ , where  $p$  is a prime such that  $p \equiv 1 \pmod{8}$  and  $p \equiv 2 \pmod{3}$  and  $n$  is a positive integer. Using the same arguments as in Sections 4 and 6, there should exist certain families of generalized Mordell curves and of generalized Fermat curves that are counterexamples to the Hasse principle explained by the Brauer-Manin obstruction. Since we will construct infinitely many generalized Mordell curves and infinitely many Fermat curves violating the Hasse principle in Sections 4 and 6, we will restrict ourselves to only describing another infinite subset of  $\mathcal{X}_p(\mathbb{Q})$  in the last section that should produce infinitely many septuples satisfying Hypothesis FM, but not proceeding to construct certain generalized Mordell curves and certain generalized Fermat curves violating the Hasse principle that arise from this subset.

## 2. NON-EXISTENCE OF RATIONAL POINTS ON CERTAIN GENERALIZED MORDELL CURVES

In this section, we describe a relationship between rational points on  $\mathcal{X}_p$  that satisfy Hypothesis FM and nonexistence of rational points on certain generalized Mordell curves. More precisely, we show that for each prime  $p \equiv 1 \pmod{8}$  and a positive integer  $n$ , the existence of a septuple  $(A, B, C, D, E, F, G)$  satisfying Hypothesis FM with respect to the couple  $(p, n)$  implies nonexistence of rational points on the generalized Mordell curve of the shape  $pz^2 = E^2x^{12n} - G^2$ . We begin by proving the main lemma in this section.

**Lemma 2.1.** *Let  $p$  be a prime such that  $p \equiv 1 \pmod{8}$ , and let  $n$  be a positive integer. Assume that  $(A, B, C, D, E, F, G) \in \mathbb{Z}^7$  is a septuple of integers satisfying Hypothesis FM with respect to the couple*

$(p, n)$ . Let  $\mathcal{C}$  be the generalized Mordell curve defined by

$$(3) \quad \mathcal{C} : pz^2 = E^2x^{12n} - G^2.$$

Let  $\mathbb{Q}(\mathcal{C})$  be the function field of  $\mathcal{C}$ , and let  $\mathcal{A}$  be the class of the quaternion algebra  $(p, A + Bx^{4n} + pz)$  in  $\text{Br}(\mathbb{Q}(\mathcal{C}))$ . Then  $\mathcal{A}$  is an Azumaya algebra of  $\mathcal{C}$ . Furthermore,  $\mathcal{B} := (p, A + Bx^{4n} - pz)$  and  $\mathcal{E} := \left(p, \frac{A + Bx^{4n} + pz}{x^{6n}}\right)$  represent the same class as  $\mathcal{A}$  in  $\text{Br}(\mathbb{Q}(\mathcal{C}))$ .

*Proof.* We will prove that there is a Zariski open covering  $(U_i)_i$  of  $\mathcal{C}$  such that  $\mathcal{A}$  extends to an element of  $\text{Br}(U_i)$  for each  $i$ .

By (A1), we see that (3) can be written in the form

$$(4) \quad (A + Bx^{4n} + pz)(A + Bx^{4n} - pz) = (Cx^{4n} + D)^2 - px^{4n}(Ex^{4n} + F)^2 \\ = \text{Norm}_{\mathbb{Q}(\sqrt{p})/\mathbb{Q}}((Cx^{4n} + D) - \sqrt{p}x^{2n}(Ex^{4n} + F)).$$

It follows from the identity above that  $\mathcal{A} + \mathcal{B} = 0$ . Furthermore, we see that  $\mathcal{A} - \mathcal{E} = (p, x^{6n}) = 0$ . Since  $\mathcal{A}, \mathcal{B}$  and  $\mathcal{E}$  belong to the 2-torsion part of  $\text{Br}(\mathbb{Q}(\mathcal{C}))$ , we deduce that  $\mathcal{A} = \mathcal{B} = \mathcal{E}$ .

Let  $U_1$  be the *largest* open subvariety of  $\mathcal{C}$  in which the rational function  $R_1 := A + Bx^{4n} + pz$  has neither a zero nor pole. Let  $U_2$  be the *largest* open subvariety of  $\mathcal{C}$  in which  $R_2 := A + Bx^{4n} - pz$  has neither a zero nor pole. Since  $\mathcal{A} = \mathcal{B}$ ,  $\mathcal{A}$  is an Azumaya algebra on  $U_1$  and also on  $U_2$ . We prove that in the affine part of  $\mathcal{C}$ , the locus where both of  $R_1$  and  $R_2$  have a zero is empty. Assume the contrary, and let  $(X, Z)$  be a common zero of  $R_1$  and  $R_2$ . We see that

$$A + BX^{4n} = R_1 + R_2 = 0$$

and

$$Z = \frac{R_1 - R_2}{2p} = 0.$$

This implies that  $B \neq 0$ ; otherwise, we deduce that  $A = 0$ , which is a contradiction to Remark 1.3. Hence  $B \neq 0$ , and thus it follows that  $X^{4n} = -\frac{A}{B}$ . By (3), we deduce that

$$X^{12n} = \frac{G^2}{E^2} = \left(-\frac{A}{B}\right)^3.$$

Hence

$$(5) \quad (-A)^3 = \frac{B^3G^2}{E^2}.$$

Let  $H$  be an integer satisfying (A5) in Definition 1.1. Since  $E \not\equiv 0 \pmod{p}$ , it follows from (A5) and (5) that

$$(-A)^3 = \frac{B^3G^2}{E^2} \equiv (BH^4)^3 \pmod{p}.$$

Hence  $-A \equiv \zeta BH^4 \pmod{p}$  for some cube root of unity  $\zeta$  in  $\mathbb{F}_p^\times$ . Thus  $A + \zeta BH^4 \equiv 0 \pmod{p}$ , which is a contradiction to (A5). Therefore, in the affine part of  $\mathcal{C}$ , the locus where both of  $R_1$  and  $R_2$  have a zero is empty.

Let  $R_3 := \frac{A + Bx^{4n} + pz}{x^{6n}}$ , and let  $\infty = (X_\infty : Y_\infty : Z_\infty)$  be a point at infinity on  $\mathcal{C}$ . We know that  $Y_\infty = 0$  and

$$\frac{Z_\infty}{X_\infty^{6n}} = \pm \frac{E}{\sqrt{p}}.$$

It follows that

$$R_3(\infty) = \frac{AY_\infty^{6n} + BX_\infty^{4n}Y_\infty^{2n} + pZ_\infty}{X_\infty^{6n}} = \frac{pZ_\infty}{X_\infty^{6n}} = \pm \sqrt{p}E.$$

By Remark 1.3, we know that  $E$  is nonzero. Hence  $R_3 \neq 0$ , and thus  $R_3$  is regular and non-vanishing at the points at infinity on  $\mathcal{C}$ .



Let  $U_3$  be the *largest* open subvariety of  $\mathcal{C}$  in which the rational function  $R_3$  has neither a zero nor pole. Then, since  $\mathcal{A} = \mathcal{E}$ , we deduce that  $\mathcal{A}$  is an Azumaya algebra on  $U_3$ . By what we have shown, it follows that  $\mathcal{C} = U_1 \cup U_2 \cup U_3$ . Since  $\mathcal{A}$  is an Azumaya algebra on each  $U_i$  for  $1 \leq i \leq 3$ , we deduce that  $\mathcal{A}$  belongs to  $\text{Br}(\mathcal{C})$ , proving our contention.  $\square$

We now prove the main theorem in this section, which relates rational points on  $\mathcal{X}_p$  satisfying Hypothesis FM to nonexistence of rational points on certain generalized Mordell curves.

**Theorem 2.2.** *Let  $p$  be a prime such that  $p \equiv 1 \pmod{8}$ , and let  $n$  be a positive integer. Let  $(A, B, C, D, E, F, G) \in \mathbb{Z}^7$  be a septuple of integers satisfying Hypothesis FM with respect to  $(p, n)$ . Let  $\mathcal{C}$  be the generalized Mordell curve defined by (3) in Lemma 2.1. Then  $\mathcal{C}(\mathbb{A}_{\mathbb{Q}})^{\text{Br}} = \emptyset$ .*

*Proof.* We maintain the notation of Lemma 2.1. We will prove that for any  $P_l \in \mathcal{C}(\mathbb{Q}_l)$ ,

$$(6) \quad \text{inv}_l(\mathcal{A}(P_l)) = \begin{cases} 0 & \text{if } l \neq p, \\ 1/2 & \text{if } l = p. \end{cases}$$

Since  $\mathcal{C}$  is smooth, we know that  $\mathcal{C}^*(\mathbb{Q}_l)$  is  $l$ -adically dense in  $\mathcal{C}(\mathbb{Q}_l)$ , where  $\mathcal{C}^*$  is the affine curve given by  $pz^2 = E^2x^{12n} - G^2$ . Since  $\text{inv}_l(\mathcal{A}(P_l))$  is a continuous function on  $\mathcal{C}(\mathbb{Q}_l)$  with respect to the  $l$ -adic topology, it suffices to prove (6) for any  $P_l \in \mathcal{C}^*(\mathbb{Q}_l)$ .

Suppose that  $l = 2, \infty$  or  $l$  is an odd prime such that  $l \neq p$  and  $p$  is a square in  $\mathbb{Q}_l^\times$ . Then, for any  $t \in \mathbb{Q}_l^\times$ , the local Hilbert symbol  $(p, t)_l$  is 1. Thus  $\text{inv}_l(\mathcal{A}(P_l))$  is 0.

Suppose that  $l = 3$ . If 3 is a square in  $\mathbb{F}_p^\times$ , then by the quadratic reciprocity law, we know that  $p$  is a square in  $\mathbb{F}_3^\times$ . Hence, using the same arguments as above, we deduce that  $\text{inv}_3(\mathcal{A}(P_3)) = 0$ . If 3 is a quadratic non-residue in  $\mathbb{F}_p^\times$ , then we contend that  $v_3(x) \geq 0$ . Assume the contrary, that is,  $v_3(x) = \epsilon < 0$ . Since  $\epsilon = v_3(x) \in \mathbb{Z}$ , we see that  $\epsilon \leq -1$ . Hence, by (A6), we deduce that

$$v_3(E^2x^{12n}) = 2v_3(E) + 12n\epsilon \leq 2v_3(E) - 12n < 2v_3(G) = v_3(G^2).$$

It then follows that

$$2v_3(z) = v_3(pz^2) = \min(v_3(E^2x^{12n}), v_3(G^2)) = v_3(E^2x^{12n}) = 2v_3(E) + 12n\epsilon,$$

and hence  $v_3(z) = v_3(E) + 6n\epsilon$ . Therefore there exist elements  $x_0, z_0, E_0 \in \mathbb{Z}_3^\times$  such that

$$\begin{aligned} x &= 3^\epsilon x_0, \\ z &= 3^{v_3(E) + 6n\epsilon} z_0, \\ E &= 3^{v_3(E)} E_0. \end{aligned}$$

By (3), we deduce that

$$p3^{2v_3(E) + 12n\epsilon} z_0^2 = 3^{2v_3(E) + 12n\epsilon} E_0^2 x_0^{12n} - G^2.$$

Multiplying both sides of the above equation by  $3^{-2v_3(E) - 12n\epsilon}$ , we see that

$$(7) \quad pz_0^2 = E_0^2 x_0^{12n} - 3^{-2v_3(E) - 12n\epsilon} G^2.$$

We see that

$$\begin{aligned} v_3(3^{-2v_3(E) - 12n\epsilon} G^2) &= 2v_3(G) - 2v_3(E) - 12n\epsilon > -12n - 12n\epsilon \quad (\text{by (A6)}) \\ &= 12n(-\epsilon - 1) \geq 0. \end{aligned}$$

Hence  $v_3(3^{-2v_3(E) - 12n\epsilon} G^2) > 0$ . Since  $v_3(3^{-2v_3(E) - 12n\epsilon} G^2)$  is an integer, it follows that

$$v_3(3^{-2v_3(E) - 12n\epsilon} G^2) \geq 1,$$

and thus  $3^{-2v_3(E) - 12n\epsilon} G^2 \in 3\mathbb{Z}_3$ . Reducing equation (7) modulo 3, we deduce that

$$p \equiv \left( \frac{E_0 x_0^{6n}}{z_0} \right)^2 \pmod{3},$$

which is a contradiction since  $p$  is not a square in  $\mathbb{F}_3^\times$ . This contradiction implies that  $v_3(x) \geq 0$ . By (3), we see that  $v_3(z) \geq 0$ .

By (A7) and (3), we deduce that

$$pz^2 = E^2x^{12n} - G^2 \equiv E^2x^{12n} \pmod{3}.$$

Since  $p$  is not a square in  $\mathbb{F}_3^\times$ , it follows that  $z \equiv Ex \equiv 0 \pmod{3}$ . Assume that  $A + Bx^{4n} + pz \equiv 0 \pmod{3}$ . Since  $z \equiv 0 \pmod{3}$ , it follows that  $A + Bx^{4n} \equiv 0 \pmod{3}$ . We see from (4) that

$$(Cx^{4n} + D)^2 - px^{4n}(Ex^{4n} + F)^2 \equiv 0 \pmod{3}.$$

Since  $p$  is not a square in  $\mathbb{F}_3^\times$ , it follows that

$$Cx^{4n} + D \equiv x(Ex^{4n} + F) \equiv 0 \pmod{3}.$$

Thus we deduce that  $A + Bx^{4n} \equiv Cx^{4n} + D \equiv 0 \pmod{3}$ . We contend that  $x \not\equiv 0 \pmod{3}$ ; otherwise,  $A \equiv D \equiv 0 \pmod{3}$ , and hence it follows from (A7) that 3 divides  $\gcd(A, D, G)$ , which is a contradiction to (A3). Thus  $x \not\equiv 0 \pmod{3}$ , and hence we deduce that  $x^2 \equiv 1 \pmod{3}$ . By (A7), we see that

$$0 \equiv A + Bx^{4n} \equiv A + B \not\equiv 0 \pmod{3},$$

which is a contradiction. Hence  $A + Bx^{4n} + pz \not\equiv 0 \pmod{3}$ , and thus we deduce that the local Hilbert symbol  $(p, A + Bx^{4n} + pz)_3$  is 1. Therefore  $\text{inv}_3(\mathcal{A}(P_3))$  is 0.

Suppose that  $l$  is an odd prime such that  $\gcd(l, 3) = \gcd(l, p) = 1$  and  $p$  is not a square in  $\mathbb{Q}_l^\times$ . We consider the following two cases.

★ *Case 1.*  $v_l(x) \geq 0$ .

Assume that

$$(8) \quad \begin{cases} A + Bx^{4n} + pz & \equiv 0 \pmod{l}, \\ A + Bx^{4n} - pz & \equiv 0 \pmod{l}. \end{cases}$$

By (4), we deduce that

$$(Cx^{4n} + D)^2 - px^{4n}(Ex^{4n} + F)^2 \equiv 0 \pmod{l}.$$

Since  $p$  is not a square in  $\mathbb{Q}_l^\times$ , it follows that

$$(9) \quad \begin{cases} Cx^{4n} + D & \equiv 0 \pmod{l}, \\ x(Ex^{4n} + F) & \equiv 0 \pmod{l}. \end{cases}$$

Adding both of the equations of (8), we deduce that

$$(10) \quad A + Bx^{4n} \equiv 0 \pmod{l}.$$

If  $x \equiv 0 \pmod{l}$ , then it follows from (10) and the first equation of (9) that  $A \equiv D \equiv 0 \pmod{l}$ . By (A1), we deduce that  $pG^2 = D^2 - A^2 \equiv 0 \pmod{l}$ . Since  $p \neq l$ , we deduce that  $l$  divides  $G$ , and hence  $l$  divides  $\gcd(A, D, G)$ , which is a contradiction to (A3). If  $x \not\equiv 0 \pmod{l}$ , then it follows from the second equation of (9) that

$$(11) \quad Ex^{4n} + F \equiv 0 \pmod{l}.$$

Hence it follows from (10), (11) and the first equation of (9) that

$$\begin{cases} BCx^{4n} & \equiv -AC \equiv -BD \pmod{l}, \\ BEx^{4n} & \equiv -AE \equiv -BF \pmod{l}, \\ CEx^{4n} & \equiv -DE \equiv -CF \pmod{l}. \end{cases}$$

Thus

$$\begin{cases} AC - BD & \equiv 0 \pmod{l}, \\ AE - BF & \equiv 0 \pmod{l}, \\ DE - CF & \equiv 0 \pmod{l}, \end{cases}$$



and hence  $l$  divides  $\gcd(AC - BD, DE - CF, AE - BF)$ . Thus it follows from (A4) that  $p$  is a square in  $\mathbb{Q}_l^\times$ , which is a contradiction. Therefore at least one of  $A + Bx^{4n} + pz$  and  $A + Bx^{4n} - pz$  is nonzero modulo  $l$ , say  $U$ . Since  $\mathcal{A}$  and  $\mathcal{B}$  represent the same class in  $\text{Br}(\mathbb{Q}(\mathcal{C}))$ , we deduce that the local Hilbert symbol  $(p, U)_l$  is 1. Hence  $\text{inv}_l(\mathcal{A}(P_l))$  is 0.

★ *Case 2.*  $v_l(x) = \epsilon < 0$ .

Since  $\epsilon = v_l(x) \in \mathbb{Z}$ , we deduce that  $\epsilon \leq -1$ . If  $v_l(E) = 0$ , then we see that

$$v_l(E^2 x^{12n}) = 12n\epsilon \leq -12n < v_l(G^2).$$

If  $v_l(E) > 0$ , then  $l$  divides  $E$ . Since  $p$  is not a square in  $\mathbb{Q}_l^\times$ , it follows from (A2) that

$$v_l(E) - v_l(G) < 6n.$$

Hence

$$v_l(E^2 x^{12n}) = 2v_l(E) + 12n\epsilon \leq 2v_l(E) - 12n < 2v_l(G) = v_l(G^2).$$

Thus, in any event, we see that  $v_l(E^2 x^{6n}) < v_l(G^2)$ . Hence it follows from (3) that

$$v_l(z) = \frac{v_l(pz^2)}{2} = \frac{\min(v_l(E^2 x^{12n}), v_l(G^2))}{2} = v_l(E) + 6n\epsilon.$$

Hence there are elements  $x_0, z_0, E_0 \in \mathbb{Z}_l^\times$  such that

$$\begin{aligned} x &= l^\epsilon x_0, \\ z &= l^{v_l(E) + 6n\epsilon} z_0, \\ E &= l^{v_l(E)} E_0. \end{aligned}$$

Hence it follows from (3) that

$$pl^{2v_l(E) + 12n\epsilon} z_0^2 = l^{2v_l(E) + 12n\epsilon} E_0^2 x_0^{12n} - G^2.$$

Multiplying both sides of the above equation by  $l^{-2v_l(E) - 12n\epsilon}$ , we deduce that

$$(12) \quad pz_0^2 = E_0^2 x_0^{12n} - G^2 l^{-2v_l(E) - 12n\epsilon}.$$

If  $v_l(E) = 0$ , then we see that

$$v_l(G^2 l^{-2v_l(E) - 12n\epsilon}) = 2v_l(G) - 2v_l(E) - 12n\epsilon = 2v_l(G) - 12n\epsilon \geq 2v_l(G) + 12n \geq 12n \geq 12.$$

If  $v_l(E) > 0$ , then we know that  $l$  divides  $E$ . Since  $p$  is not a square in  $\mathbb{Q}_l^\times$ , we deduce from (A2) that

$$v_l(E) - v_l(G) < 6n,$$

and hence

$$\begin{aligned} v_l(G^2 l^{-2v_l(E) - 12n\epsilon}) &= 2v_l(G) - 2v_l(E) - 12n\epsilon \\ &> -12n - 12n\epsilon = 12n(-\epsilon - 1) \geq 0. \end{aligned}$$

Thus, in any event, we see that

$$v_l(G^2 l^{-2v_l(E) - 12n\epsilon}) > 0.$$

Since  $v_l(G^2 l^{-2v_l(E) - 12n\epsilon})$  is an integer, it follows that  $v_l(G^2 l^{-2v_l(E) - 12n\epsilon}) \geq 1$ , and hence

$$G^2 l^{-2v_l(E) - 12n\epsilon} \in l\mathbb{Z}_l.$$

Reducing equation (12) modulo  $l$ , one obtains that

$$p \equiv \left( \frac{E_0 x_0^{6n}}{z_0} \right)^2 \pmod{l},$$

which is a contradiction since  $p$  is not a square in  $\mathbb{Q}_l^\times$ .

Thus, in any event, if  $l$  is an odd prime such that  $\gcd(l, 3) = \gcd(l, p) = 1$  and  $p$  is not a square in  $\mathbb{Q}_l^\times$ , then  $\text{inv}_l(\mathcal{A}(P_l))$  is 0.

Suppose that  $l = p$ . If  $v_p(x) = \epsilon < 0$ , then we know from (A3) that  $E \not\equiv 0 \pmod{p}$ . Hence we see that

$$v_p(E^2 x^{12n}) = 12n\epsilon < 0 \leq v_p(G^2).$$

It then follows from the above inequality and (3) that

$$1 + 2v_p(z) = v_p(pz^2) = v_p(E^2 x^{12n}) = 12n\epsilon,$$

which is a contradiction since the left-hand side is an odd integer whereas the right-hand side is an even integer.

If  $v_p(x) \geq 0$ , then it follows from (3) that

$$1 + 2v_p(z) = v_p(pz^2) = v_p(E^2 x^{12n} - G^2) \geq 0.$$

Hence it follows that  $v_p(z) \geq -\frac{1}{2}$ . Since  $v_p(z) \in \mathbb{Z}$ , we deduce that  $v_p(z) \geq 0$ , and hence  $z \in \mathbb{Z}_p$ . We contend that  $x \in \mathbb{Z}_p^\times$ . Assume the contrary, that is,  $x \equiv 0 \pmod{p}$ . By (3), we deduce that

$$G^2 = E^2 x^{12n} - pz^2 \equiv 0 \pmod{p},$$

which is a contradiction to (A3). Hence we deduce that  $x \in \mathbb{Z}_p^\times$ . Reducing equation (3) modulo  $p$ , we deduce that

$$(13) \quad E^2 x^{12n} - G^2 \equiv 0 \pmod{p}.$$

Let  $H$  be an integer satisfying (A5) in Definition 1.1. By (13), (A3) and (A5), we see that

$$x^{12n} \equiv \left(\frac{G}{E}\right)^2 \equiv H^{12} \pmod{p},$$

and hence  $x^{4n} \equiv \zeta H^4 \pmod{p}$  for some cube root of unity  $\zeta$  in  $\mathbb{F}_p^\times$ . Thus it follows from (A5) that

$$A + Bx^{4n} + pz \equiv A + \zeta BH^4 \not\equiv 0 \pmod{p}.$$

Using Theorem 5.2.7 in [2], we deduce from (A5) that the local Hilbert symbol  $(p, A + Bx^{4n} + pz)_p$  satisfies

$$(p, A + Bx^{4n} + pz)_p = \left(\frac{A + \zeta BH^4}{p}\right) = -1,$$

which proves that  $\text{inv}_p(\mathcal{A}(P_p)) = 1/2$ .

Therefore, in any event, we have

$$\sum_l \text{inv}_l \mathcal{A}(P_l) = 1/2$$

for any  $(P_l)_l \in \mathcal{C}(\mathbb{A}_{\mathbb{Q}})$ , and hence  $\mathcal{C}(\mathbb{A}_{\mathbb{Q}})^{\text{Br}} = \emptyset$ . Hence our contention follows.  $\square$

### 3. A SUBSET OF THE SET OF ALL RATIONAL POINTS ON $\mathcal{X}_p$

Let  $p$  be a prime such that  $p \equiv 1 \pmod{8}$  and  $p \equiv 2 \pmod{3}$ . Let  $n$  be an integer such that  $n \geq 2$ . In this section, we will construct a subset of the set of all rational points on  $\mathcal{X}_p$  that produces infinitely many septuples  $(A, B, C, D, E, F, G) \in \mathbb{Z}^7$  satisfying Hypothesis FM with respect to  $(p, n)$  in the sense of Definition 1.1. This subset of  $\mathcal{X}_p(\mathbb{Q})$  plays a key role in constructing certain families of generalized Mordell curves and certain families of generalized Fermat curves that are counterexamples to the Hasse principle explained by the Brauer-Manin obstruction.

Let  $(\alpha, \beta, \kappa) \in \mathbb{Z}^3$  be a triple of nonzero integers satisfying the following conditions:

- (B1)  $\alpha$  and  $\beta$  are odd and  $\gcd(\alpha, 3) = \gcd(\alpha, p) = \gcd(\alpha, \beta) = \gcd(\beta, p) = 1$ .
- (B2) let  $l$  be any odd prime such that  $\gcd(l, 3) = 1$  and  $l$  divides  $\alpha\beta$ . Then  $p$  is a square in  $\mathbb{Q}_l^\times$ .
- (B3)  $v_3(\kappa) < 2n - 1$  and  $v_3(\kappa)$  is an odd positive integer.
- (B4)  $\kappa \not\equiv 0 \pmod{p}$ .
- (B5) let  $l$  be any odd prime such that  $\gcd(l, 3) = 1$  and  $l$  divides  $\kappa$ . Then  $p$  is a square in  $\mathbb{Q}_l^\times$ .

Define

$$(14) \quad \begin{cases} A &:= \frac{p\alpha^2 - 9\beta^2}{2} \\ B &:= 9(p\alpha^2 - 9\beta^2)\kappa^2 \\ C &:= 9(p\alpha^2 + 9\beta^2)\kappa^2 \\ D &:= \frac{p\alpha^2 + 9\beta^2}{2} \\ E &:= 81\alpha\beta\kappa^3 \\ F &:= 18\alpha\beta\kappa \\ G &:= 3\alpha\beta. \end{cases}$$

By (14), we deduce that

$$(15) \quad \begin{cases} B &= 18\kappa^2 A \\ C &= 18\kappa^2 D \\ E &= 27\kappa^3 G \\ F &= 6\kappa G. \end{cases}$$

We now prove that  $(A, B, C, D, E, F, G)$  satisfies Hypothesis FM with respect to  $(p, n)$ .

**Lemma 3.1.** *Let  $p$  be a prime such that  $p \equiv 1 \pmod{8}$  and  $p \equiv 2 \pmod{3}$ . Let  $n$  be an integer such that  $n \geq 2$ . Let  $(\alpha, \beta, \kappa) \in \mathbb{Z}^3$  be a triple of nonzero integers satisfying (B1) – (B5). Let  $\mathcal{T} := (A, B, C, D, E, F, G) \in \mathbb{Z}^7$  be a septuple of integers defined by (14). Then  $\mathcal{T}$  satisfies Hypothesis FM with respect to  $(p, n)$ .*

*Proof.* By (B1), (B4) and (14), we see that  $\mathcal{T}$  satisfies (A3) and (A7). Furthermore, it is not difficult to verify that the point  $\mathcal{P} := (a : b : c : d : e : f : g) = (A : B : C : D : E : F : G)$  belongs to  $\mathcal{X}_p(\mathbb{Q})$ , and hence  $\mathcal{T}$  satisfies (A1).

We now prove that  $\mathcal{T}$  satisfies (A2). Indeed, let  $l$  be an odd prime such that  $\gcd(l, 3) = \gcd(l, p) = 1$  and  $l$  divides  $E$ . We see that either  $l$  divides  $\kappa$  or  $\gcd(l, \kappa) = 1$ . If  $l$  divides  $\kappa$ , then it follows from (B5) that  $p$  is a square in  $\mathbb{Q}_l^\times$ . Assume that  $\gcd(l, \kappa) = 1$ . By (15), we see that

$$v_l(E) - v_l(G) = v_l(27\kappa^3 G) - v_l(G) = v_l(27\kappa^3) = 0 < 6n,$$

and hence  $\mathcal{T}$  satisfies (A2).

We now prove that  $\mathcal{T}$  satisfies (A4). Suppose that  $l$  is an odd prime such that  $\gcd(l, 3) = \gcd(l, p) = 1$  and

$$\gcd(AC - BD, DE - CF, AE - BF) \equiv 0 \pmod{l}.$$

By (B1) and (14), one can show that  $\gcd(A, D) = 1$ . By (15), we see that

$$\begin{aligned} AC - BD &= 0, \\ DE - CF &= -3^4\kappa^3 DG, \\ AE - BF &= -3^4\kappa^3 AG. \end{aligned}$$

Hence it follows that

$$\gcd(AC - BD, DE - CF, AE - BF) = \pm 3^4\kappa^3 G,$$

and hence we deduce that  $l$  divides  $3^4\kappa^3 G$ . Since  $\gcd(l, 3) = 1$ , it follows from (14) that  $l$  divides  $\kappa$  or  $\alpha\beta$ . By (B2) and (B5), we deduce that  $p$  is a square in  $\mathbb{Q}_l^\times$ , which proves that (A4) is true.

We now prove that (A5) holds. Let  $\kappa^*$  be the integer such that  $\kappa = 3^{v_3(\kappa)}\kappa^*$  and  $\gcd(\kappa^*, 3) = 1$ , where  $v_3$  denotes the 3-adic valuation. We contend that  $3\kappa$  is a square in  $\mathbb{F}_p^\times$ . Indeed, we see that  $3\kappa = 3^{v_3(\kappa)+1}\kappa^*$ . By (B3), we deduce that  $v_3(\kappa) + 1$  is an even positive integer, and hence it follows that  $3^{v_3(\kappa)+1}$  is a square in  $\mathbb{F}_p^\times$ . Thus it suffices to show that  $\kappa^*$  is a square in  $\mathbb{F}_p^\times$ . Write  $\kappa^* = \pm 2^{v_2(\kappa^*)} \prod_{l|\kappa^*} l^{v_l(\kappa^*)}$ , where  $l$  ranges over the set of all odd primes dividing  $\kappa^*$ . By (B5) and the

quadratic reciprocity law, we know that  $l$  is a square in  $\mathbb{F}_p^\times$  for any odd prime  $l$  dividing  $\kappa^*$ . Since  $p \equiv 1 \pmod{8}$ , we deduce that the Jacobi symbol  $\left(\frac{\kappa^*}{p}\right)$  satisfies

$$\left(\frac{\kappa^*}{p}\right) = \left(\frac{\pm 1}{p}\right) \left(\frac{2^{v_2(\kappa^*)}}{p}\right) \left(\prod_{l|\kappa^*} \left(\frac{l}{p}\right)\right) = 1.$$

Thus  $\kappa^*$  is a square in  $\mathbb{F}_p^\times$ , and hence  $3\kappa$  is a square in  $\mathbb{F}_p^\times$ . Thus there exists an integer  $H$  such that

$$(16) \quad 3\kappa H^2 \equiv 1 \pmod{p}.$$

We contend that  $H$  satisfies (A5). Indeed, by (15) and (16), we see that

$$G - EH^6 = G - 27\kappa^3 GH^6 = G(1 - 27\kappa^3 H^6) = G(1 - (3\kappa H^2)^3) \equiv 0 \pmod{p}.$$

By Remark 1.2 and since  $p \equiv 2 \pmod{3}$ , it remains to show that  $A + BH^4$  is a quadratic non-residue in  $\mathbb{F}_p^\times$ . By (15) and (16), we know that

$$A + BH^4 = A + 18\kappa^2 AH^4 = A(1 + 18\kappa^2 H^4) = A(1 + 2(3\kappa H^2)^2) \equiv 3A \pmod{p}.$$

By (14), we see that

$$3A = \frac{3(p\alpha^2 - 9\beta^2)}{2} \equiv -\frac{3(3\beta)^2}{2} \pmod{p}.$$

Since  $p \equiv 1 \pmod{8}$ , we know that  $-1$  and  $1/2$  are squares in  $\mathbb{F}_p^\times$ . Since  $p \equiv 2 \pmod{3}$ , we see that  $p$  is a quadratic non-residue modulo 3, and it follows from the quadratic reciprocity law that 3 is not a square in  $\mathbb{F}_p^\times$ . Thus we deduce that the Jacobi symbol  $\left(\frac{A + BH^4}{p}\right)$  satisfies

$$\left(\frac{A + BH^4}{p}\right) = \left(\frac{3A}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{1/2}{p}\right) \left(\frac{3}{p}\right) \left(\frac{(3\beta)^2}{p}\right) = -1,$$

and thus  $A + BH^4$  is a quadratic non-residue in  $\mathbb{F}_p^\times$ . Therefore  $\mathcal{T}$  satisfies (A5).

By (B3) and (15), we know that

$$v_3(E) - v_3(G) = v_3(27\kappa^3 G) - v_3(G) = v_3(27) + v_3(\kappa^3) = 3 + 3v_3(\kappa) < 6n,$$

and hence  $\mathcal{T}$  satisfies (A6). Thus our contention follows.  $\square$

**Corollary 3.2.** *Let  $p$  be a prime such that  $p \equiv 1 \pmod{8}$  and  $p \equiv 2 \pmod{3}$ . Let  $n$  be an integer such that  $n \geq 2$ . Let  $\kappa$  be a nonzero integer satisfying (B3), (B4) and (B5). Let  $\mathcal{D}$  be the smooth projective model of the affine curve defined by*

$$(17) \quad \mathcal{D} : pz^2 = 3^6 \kappa^6 x^{12n} - 1.$$

*Then  $\mathcal{D}(\mathbb{A}_{\mathbb{Q}})^{\text{Br}} = \emptyset$ .*

*Proof.* It is easy to show that there are infinitely many couples  $(\alpha, \beta) \in \mathbb{Z}^2$  of nonzero integers that satisfy (B1) and (B2). Take such a couple  $(\alpha, \beta) \in \mathbb{Z}^2$ , and let  $\mathcal{T} := (A, B, C, D, E, F, G) \in \mathbb{Z}^7$  be the septuple of integers defined by (14). It follows from Lemma 3.1 that  $\mathcal{T}$  satisfies Hypothesis FM with respect to  $(p, n)$ . Let  $\mathcal{C}$  be the smooth projective model of the affine curve defined by (3) in Theorem 2.2, that is,  $\mathcal{C}$  is of the form

$$\mathcal{C} : pz^2 = E^2 x^{12n} - G^2.$$

By Theorem 2.2, we know that  $\mathcal{C}(\mathbb{A}_{\mathbb{Q}})^{\text{Br}} = \emptyset$ . By (15), we know that  $E = 3^3 \kappa^3 G$ . Hence, under the morphism

$$(x, z) \mapsto (x, Gz),$$

we see that the curve  $\mathcal{C}$  is isomorphic to  $\mathcal{D}$  over  $\mathbb{Q}$ . Thus we deduce that  $\mathcal{D}(\mathbb{A}_{\mathbb{Q}})^{\text{Br}} = \emptyset$ .  $\square$

## 4. CERTAIN GENERALIZED MORDELL CURVES VIOLATING THE HASSE PRINCIPLE

Let  $p$  be an odd prime such that  $p \equiv 1 \pmod{8}$  and  $p \equiv 2 \pmod{3}$ . Let  $n$  be an integer such that  $n \geq 2$ . Let  $\kappa$  be a nonzero integer satisfying (B3), (B4) and (B5). In this section, we will prove a sufficient condition depending on certain congruences of  $\kappa$  modulo finitely many primes under which the curve  $\mathcal{D}$  defined by (17) is a counterexample to the Hasse principle explained by the Brauer-Manin obstruction. This result will be proved in Subsection 4.1. As a consequence, in Subsection 4.2, we will show that there are infinitely many integers  $\kappa$  satisfying the sufficient condition, and hence it follows that there are infinitely many non-isomorphic generalized Mordell curves violating the Hasse principle explained by the Brauer-Manin obstruction.

**4.1. A sufficient condition.** We recall the celebrated *Hasse-Weil bound*.

**Lemma 4.1.** (see [8, Corollary 7.2.1, p.130])

Let  $\mathcal{X}$  be a smooth geometrically irreducible projective curve of genus  $n$  over the finite field  $\mathbb{F}_q$ . Then

$$|\#\mathcal{X}(\mathbb{F}_q) - (q + 1)| \leq 2n\sqrt{q}.$$

We now prove the main theorem in this section.

**Theorem 4.2.** Let  $p$  be a prime such that  $p \equiv 1 \pmod{8}$  and  $p \equiv 2 \pmod{3}$ . Let  $n$  be an integer such that  $n \geq 2$ . Let  $\kappa$  be a nonzero integer satisfying (B3), (B4) and (B5). Assume further that the following are true:

(C1)  $\kappa \equiv \frac{1}{3} \pmod{p^{2v_p(n)+1}}.$

(C2) let  $\mathbf{A}$  be the set of odd primes  $l$  satisfying the following three conditions:

(i)  $\gcd(l, 3) = \gcd(l, p) = \gcd(l, \kappa) = 1.$

(ii)  $\left(\frac{p}{l}\right) = \left(\frac{-p}{l}\right) = -1.$

(iii)  $l$  divides  $n$ .

We assume that  $3^6\kappa^6 - 1$  is a quadratic non-residue in  $\mathbb{F}_l^\times$  or  $\kappa \equiv \frac{1}{3} \pmod{l^{2v_l(n)+1}}$  for each prime  $l \in \mathbf{A}$ .

(C3) let  $\mathbf{B}$  be the set of odd primes  $l$  satisfying the following three conditions:

(i)  $\gcd(l, 3) = \gcd(l, p) = \gcd(l, \kappa) = \gcd(l, n) = 1.$

(ii)  $\left(\frac{p}{l}\right) = \left(\frac{-p}{l}\right) = -1.$

(iii)  $l \leq 4(6n - 1)^2.$

We assume that  $3^6\kappa^6 - 1$  is a quadratic non-residue in  $\mathbb{F}_l^\times$  or  $\kappa \equiv \frac{1}{3} \pmod{l}$  for each prime  $l \in \mathbf{B}$ .

Let  $\mathcal{D}$  be the smooth projective model of the affine curve defined by (17) in Corollary 3.2. Then  $\mathcal{D}$  is a counterexample to the Hasse principle explained by the Brauer-Manin obstruction.

*Proof.* By Corollary 3.2, we know that  $\mathcal{D}(\mathbb{A}_{\mathbb{Q}})^{\text{Br}} = \emptyset$ . Hence it remains to prove that  $\mathcal{D}$  is everywhere locally solvable.

Let  $\mathbf{S}_1$  be the set of odd primes  $l$  with  $\gcd(l, p) = 1$  such that  $\left(\frac{p}{l}\right) = 1$  or  $\left(\frac{-p}{l}\right) = 1$ . Let  $\mathbf{S}_2$  be the set of odd primes  $l$  with  $\gcd(l, p) = 1$  such that  $\left(\frac{p}{l}\right) = \left(\frac{-p}{l}\right) = -1$ . Since  $-p \equiv -2 \equiv 1 \pmod{3}$ , we see that 3 belongs to  $\mathbf{S}_1$ . By (B5), we also know that if  $l$  is any odd prime such that  $\gcd(l, 3) = 1$  and  $l$  divides  $\kappa$ , then  $l$  belongs to  $\mathbf{S}_1$ . We know that

$$\{\text{the set of all primes}\} = \{2\} \cup \{p\} \cup \mathbf{S}_1 \cup \mathbf{S}_2.$$

It suffices to consider the following cases.

★ *Case 1.*  $l = p$ .

We consider the system of equations

$$(18) \quad \begin{cases} F(x, z) := 3^6 \kappa^6 x^{12n} - 1 - pz^2 & \equiv 0 \pmod{p^{2v_p(n)+1}} \\ \frac{\partial F}{\partial x}(x, z) = 2^2 3^7 \kappa^6 n x^{12n-1} & \equiv 0 \pmod{p^{v_p(n)}} \\ \frac{\partial F}{\partial x}(x, z) & \not\equiv 0 \pmod{p^{v_p(n)+1}}. \end{cases}$$

By (C1), we see that

$$F(1, 0) = (3\kappa)^6 - 1 \equiv 0 \pmod{p^{2v_p(n)+1}}.$$

Since  $p \neq 2, 3$  and  $\gcd(\kappa, p) = 1$ , we deduce that

$$\begin{aligned} \frac{\partial F}{\partial x}(1, 0) &= 2^2 3^7 \kappa^6 n \equiv 0 \pmod{p^{v_p(n)}}, \\ \frac{\partial F}{\partial x}(1, 0) &= 2^2 3^7 \kappa^6 n \not\equiv 0 \pmod{p^{v_p(n)+1}}. \end{aligned}$$

Hence  $(1, 0)$  is a solution to the system (18), and it thus follows from Hensel's lemma that  $\mathcal{D}$  is locally solvable at  $p$ .

★ *Case 2.*  $l = \infty$ ,  $l = 2$  or  $l \in \mathbf{S}_1$ .

We see that the curve  $\mathcal{D}^*$  defined by

$$\mathcal{D}^* : pz^2 = 3^6 \kappa^6 x^{12n} - y^{12n}$$

is an open subscheme of  $\mathcal{D}$ . Assume first that  $l = \infty$ ,  $l = 2$  or  $l$  is an odd prime such that  $\left(\frac{p}{l}\right) = 1$ . Define

$$P_1 := (x : y : z) = (p : 0 : 3^3 \kappa^3 p^{6n-1} \sqrt{p}).$$

Since  $\sqrt{p} \in \mathbb{Q}_l^\times$ , we deduce that  $P_1 \in \mathcal{D}^*(\mathbb{Q}_l) \subseteq \mathcal{D}(\mathbb{Q}_l)$ .

Suppose now that  $l$  is an odd prime such that  $\left(\frac{-p}{l}\right) = 1$ . We define

$$P_2 := (x, z) = \left(0, \frac{\sqrt{-p}}{p}\right).$$

Since  $\sqrt{-p} \in \mathbb{Q}_l^\times$ , we deduce that  $P_2$  belongs to  $\mathcal{D}(\mathbb{Q}_l)$ . Hence, in any event,  $\mathcal{D}$  is locally solvable at  $l$ .

★ *Case 3.*  $l \in \mathbf{S}_2$ .

By the discussion preceding *Case 1*, one can assume that  $\gcd(l, 3) = \gcd(l, \kappa) = 1$ . We know that the discriminant of the curve  $\mathcal{D}$  is

$$\text{Discriminant}(\mathcal{D}) = -3^{6(12n-1)} \kappa^{6(12n-1)} p^{2(12n-1)} (12n)^{12n}.$$

Hence  $\mathcal{D}$  is only singular at the primes  $q = 2, 3, p$ , and the primes  $q$  dividing  $\kappa n$ ; so the Hasse-Weil bound (see Lemma 4.1) assures that  $\mathcal{D}$  is locally solvable at primes  $q > 4(6n-1)^2$  such that  $q \neq 2, 3, p$  and  $\gcd(q, \kappa) = \gcd(q, n) = 1$ . Hence, by *Cases 1 and 2*, we only need to prove that  $\mathcal{D}$  is locally solvable at the primes  $l$ , where  $l \in \mathbf{A}$  or  $l \in \mathbf{B}$ .

• *Subcase 1.*  $l \in \mathbf{A}$ .

Since  $l \in \mathbf{A}$ , it follows from (C2) that  $3^6 \kappa^6 - 1$  is a quadratic non-residue in  $\mathbb{F}_l^\times$  or  $\kappa \equiv \frac{1}{3} \pmod{l^{2v_l(n)+1}}$ . Assume first that  $3^6 \kappa^6 - 1$  is a quadratic non-residue in  $\mathbb{F}_l^\times$ . We consider the system of equations

$$(19) \quad \begin{cases} F(x, z) = 3^6 \kappa^6 x^{12n} - 1 - pz^2 & \equiv 0 \pmod{l} \\ \frac{\partial F}{\partial z}(x, z) = -2pz & \not\equiv 0 \pmod{l}. \end{cases}$$

Since  $l$  belongs to  $\mathbf{A}$ , we know that  $p$  is a quadratic non-residue in  $\mathbb{F}_l^\times$ . It then follows that  $\frac{3^6 \kappa^6 - 1}{p}$  is a square in  $\mathbb{F}_l^\times$ , and thus there exists an integer  $z_0$  such that  $z_0 \not\equiv 0 \pmod{l}$  and  $\frac{3^6 \kappa^6 - 1}{p} \equiv z_0^2 \pmod{l}$ . Hence we deduce that  $F(1, z_0)$  is zero modulo  $l$ . Since  $l$  does not divide  $z_0$ , it follows that

$\frac{\partial F}{\partial z}(1, z_0) = -2pz_0 \not\equiv 0 \pmod{l}$ . Thus  $(1, z_0)$  is a solution to the system (19), and therefore it follows from Hensel's lemma that  $\mathcal{D}$  is locally solvable at  $l$ .

Suppose now that  $\kappa \equiv \frac{1}{3} \pmod{l^{2v_l(n)+1}}$ . Since  $l \neq 2, 3$  and  $\gcd(l, p) = \gcd(l, \kappa) = 1$ , one can show that the point  $(1, 0)$  is a solution to the system of equations

$$\begin{cases} F(x, z) = 3^6 \kappa^6 x^{12n} - 1 - pz^2 & \equiv 0 \pmod{l^{2v_l(n)+1}} \\ \frac{\partial F}{\partial z}(x, z) = 2^2 3^7 \kappa^6 n x^{12n-1} & \equiv 0 \pmod{l^{v_l(n)}} \\ \frac{\partial F}{\partial x}(x, z) & \not\equiv 0 \pmod{l^{v_l(n)+1}}. \end{cases}$$

By Hensel's lemma, we deduce that  $\mathcal{D}$  is locally solvable at  $l$ .

• *Subcase 2.  $l \in \mathbf{B}$ .*

Since  $l \in \mathbf{B}$ , it follows from (C3) that  $3^6 \kappa^6 - 1$  is a quadratic non-residue in  $\mathbb{F}_l^\times$  or  $\kappa \equiv \frac{1}{3} \pmod{l}$ . Assume first that  $3^6 \kappa^6 - 1$  is a quadratic non-residue in  $\mathbb{F}_l^\times$ . Then, using the same arguments as in *Subcase 1*, we deduce that  $\frac{3^6 \kappa^6 - 1}{p}$  is a square in  $\mathbb{F}_l^\times$ , and thus there exists an integer  $z_0$  such that  $z_0 \not\equiv 0 \pmod{l}$  and  $\frac{3^6 \kappa^6 - 1}{p} \equiv z_0^2 \pmod{l}$ . Repeating in the same manner as in *Subcase 1*, we see that  $(1, z_0)$  is a solution to the system of equations

$$\begin{cases} F(x, z) = 3^6 \kappa^6 x^{12n} - 1 - pz^2 & \equiv 0 \pmod{l} \\ \frac{\partial F}{\partial z}(x, z) = -2pz & \not\equiv 0 \pmod{l}. \end{cases}$$

By Hensel's lemma, we deduce that  $\mathcal{D}$  is locally solvable at  $l$ .

Suppose now that  $\kappa \equiv \frac{1}{3} \pmod{l}$ . Since  $l \neq 2, 3$  and  $\gcd(l, p) = \gcd(l, \kappa) = \gcd(l, n) = 1$ , one can show that the point  $(1, 0)$  is a solution to the system of equations

$$\begin{cases} F(x, z) = 3^6 \kappa^6 x^{12n} - 1 - pz^2 & \equiv 0 \pmod{l} \\ \frac{\partial F}{\partial x}(x, z) = 2^2 3^7 \kappa^6 n x^{12n-1} & \not\equiv 0 \pmod{l}. \end{cases}$$

By Hensel's lemma, we deduce that  $\mathcal{D}$  is locally solvable at  $l$ .

Therefore, in any event,  $\mathcal{D}$  is everywhere locally solvable, and hence our contention follows.  $\square$

**4.2. Infinitude of the triples  $(p, n, \kappa)$ .** In this subsection, we will prove that for a prime  $p \equiv 1 \pmod{8}$  and a positive integer  $n \geq 2$ , there are infinitely many nonzero integers  $\kappa$  satisfying the conditions in Theorem 4.2. The main result in this subsection is the following lemma.

**Lemma 4.3.** *Let  $p$  be a prime such that  $p \equiv 1 \pmod{8}$  and  $p \equiv 2 \pmod{3}$ . Let  $n$  and  $m$  be two integers such that  $n \geq 2$  and  $1 \leq m < n$ . Then, for any positive integer  $r$  dividing  $m$ , there are infinitely many nonzero integers  $\kappa$  of the form*

$$\kappa = 3^{2m-1} \kappa_*^r,$$

where  $\kappa_*$  is an odd prime with  $\gcd(\kappa_*, 3) = 1$  such that  $\kappa$  satisfies (B3) – (B5) and (C1) – (C3).

*Proof.* Let  $r$  be any positive integer such that  $r$  divides  $m$ , and define

$$s := \frac{m}{r}.$$

Let  $\mathbf{A}^*$  be the set of odd primes  $l$  satisfying the following three conditions:

- (1)  $\gcd(l, 3) = \gcd(l, p) = 1$ ,
- (2)  $\left(\frac{p}{l}\right) = \left(\frac{-p}{l}\right) = -1$ , and
- (3)  $l$  divides  $n$ .



Let  $\mathbf{B}^*$  be the set of odd primes  $l$  satisfying the following three conditions:

- (1)  $\gcd(l, 3) = \gcd(l, p) = \gcd(l, n) = 1$ ,
- (2)  $\left(\frac{p}{l}\right) = \left(\frac{-p}{l}\right) = -1$ , and
- (3)  $l \leq 4(6n-1)^2$ .

It is easy to see that  $p$  does not belong to  $\mathbf{A}^* \cup \mathbf{B}^*$  and  $\mathbf{A}^* \cap \mathbf{B}^* = \emptyset$ . We also note that  $\mathbf{A}^*$  and  $\mathbf{B}^*$  are of finite cardinality. Hence, by the Chinese Remainder Theorem, there exists an integer  $\kappa_{*,0}$  satisfying the following conditions:

- (i)  $\kappa_{*,0} \equiv \frac{1}{3^{2s}} \pmod{p^{2v_p(n)+1}}$ ,
- (ii)  $\kappa_{*,0} \equiv \frac{1}{3^{2s}} \pmod{l^{2v_l(n)+1}}$  for each prime  $l \in \mathbf{A}^*$ , and
- (iii)  $\kappa_{*,0} \equiv \frac{1}{3^{2s}} \pmod{l}$  for each prime  $l \in \mathbf{B}^*$ .

Let  $P(X) \in \mathbb{Z}[X]$  be the linear polynomial defined by

$$(20) \quad P(X) := p^{2v_p(n)+1} \left( \prod_{l \in \mathbf{A}^*} l^{2v_l(n)+1} \right) \left( \prod_{l \in \mathbf{B}^*} l \right) X + \kappa_{*,0}.$$

By (i), (ii) and (iii) above, we know that  $\gcd(\kappa_{*,0}, p) = \gcd(\kappa_{*,0}, l) = 1$  for any prime  $l \in \mathbf{A}^* \cup \mathbf{B}^*$ . Using Dirichlet's theorem on arithmetic progressions, we deduce that there are infinitely many integers  $X$  such that  $P(X) \neq 3$  and  $P(X)$  is an odd prime. Take such an integer  $X$ , and let  $\kappa_* := P(X)$ . We define

$$\kappa := 3^{2m-1} \kappa_*^r.$$

We contend that  $\kappa$  satisfies our requirements. Indeed, since  $\gcd(\kappa_*, 3) = 1$ , we see that

$$v_3(\kappa) = v_3(3^{2m-1} \kappa_*^r) = 2m-1 < 2n-1.$$

Hence  $\kappa$  satisfies (B3) in Section 3.

By (i) and (20) above, one knows that

$$(21) \quad \kappa_* = P(X) \equiv \kappa_{*,0} \equiv \frac{1}{3^{2s}} \pmod{p^{2v_p(n)+1}},$$

and hence

$$\kappa_* \equiv \left( \frac{1}{3^s} \right)^2 \not\equiv 0 \pmod{p}.$$

Thus  $\kappa_*$  is a quadratic residue in  $\mathbb{F}_p^\times$ , and therefore it follows from the quadratic reciprocity law that  $p$  is a square in  $\mathbb{F}_{\kappa_*}^\times$ . Therefore  $\kappa$  satisfies (B4) and (B5).

By (21) and the definition of  $\kappa$ , we see that

$$\kappa = 3^{2m-1} \kappa_*^r \equiv \frac{3^{2m-1}}{3^{2rs}} \equiv \frac{3^{2m-1}}{3^{2m}} \equiv \frac{1}{3} \pmod{p^{2v_p(n)+1}},$$

which proves that (C1) in Theorem 4.2 is true.

Now let  $\mathbf{A}$  and  $\mathbf{B}$  be the sets of odd primes defined as in (C2) and (C3) in Theorem 4.2. One sees that

$$\begin{aligned} \mathbf{A} &= \{l \in \mathbf{A}^* \mid \gcd(l, \kappa) = 1\} \subseteq \mathbf{A}^*, \\ \mathbf{B} &= \{l \in \mathbf{B}^* \mid \gcd(l, \kappa) = 1\} \subseteq \mathbf{B}^*. \end{aligned}$$

By (ii) and (20), we know that

$$\kappa = 3^{2m-1} \kappa_*^r \equiv 3^{2m-1} \kappa_{*,0}^r \equiv \frac{3^{2m-1}}{3^{2rs}} \equiv \frac{3^{2m-1}}{3^{2m}} \equiv \frac{1}{3} \pmod{l^{2v_l(n)+1}}$$

for any prime  $l \in \mathbf{A}^*$ . Since  $\mathbf{A} \subseteq \mathbf{A}^*$ , we deduce that  $\kappa \equiv \frac{1}{3} \pmod{l^{2v_l(n)+1}}$  for any prime  $l \in \mathbf{A}$ , and thus (C2) holds. Finally, using the same arguments as above, it follows from (iii) and (20) that  $\kappa \equiv \frac{1}{3} \pmod{l}$  for any prime  $l \in \mathbf{B}^*$ . Since  $\mathbf{B} \subseteq \mathbf{B}^*$ , we deduce that  $\kappa \equiv \frac{1}{3} \pmod{l}$  for any prime  $l \in \mathbf{B}$ , and thus (C3) is true. Therefore our contention follows.  $\square$

**Corollary 4.4.** *Let  $p$  be a prime such that  $p \equiv 1 \pmod{8}$  and  $p \equiv 2 \pmod{3}$ . Let  $n$  be an integer such that  $n \geq 2$ . Then there are infinitely many non-isomorphic generalized Mordell curves of degree  $12n$  that are counterexamples to the Hasse principle explained by the Brauer-Manin obstruction.*

*Proof.* Let  $m$  be any integer such that  $1 \leq m < n$ . Let  $r$  be any positive integer such that  $r$  divides  $m$ . Let  $\mathbf{C}$  be the set of nonzero integers  $\kappa$  satisfying the following conditions:

- (1)  $\kappa = 3^{2m-1}\kappa_*^r$  for some odd prime  $\kappa_* \neq 3$ , and
- (2)  $\kappa$  satisfies (B3) – (B5) and (C1) – (C3).

By Lemma 4.3, we know that  $\mathbf{C}$  is of infinite cardinality. For each integer  $\kappa \in \mathbf{C}$ , let  $\mathcal{D}_\kappa$  be the smooth projective model of the affine curve defined by

$$\mathcal{D}_\kappa : pz^2 = 3^6 \kappa^6 x^{12n} - 1.$$

By Theorem 4.2, we deduce that  $\mathcal{D}_\kappa$  is a counterexample to the Hasse principle explained by the Brauer-Manin obstruction for each  $\kappa \in \mathbf{C}$ . We contend that  $\mathcal{D}_{\kappa_1}$  is not isomorphic to  $\mathcal{D}_{\kappa_2}$  for any two distinct integers  $\kappa_1, \kappa_2 \in \mathbf{C}$ . Assume the contrary, that is,  $\mathcal{D}_{\kappa_1}$  is isomorphic to  $\mathcal{D}_{\kappa_2}$  for some distinct integers  $\kappa_1, \kappa_2 \in \mathbf{C}$ . Hence we deduce that the rational number  $\frac{3^6 \kappa_1^6}{3^6 \kappa_2^6}$  is a  $12n$ -th power. Since  $\kappa_1$  and  $\kappa_2$  are in  $\mathbf{C}$ , we can write

$$\begin{aligned} \kappa_1 &= 3^{2m-1} \kappa_{*,1}^r, \\ \kappa_2 &= 3^{2m-1} \kappa_{*,2}^r, \end{aligned}$$

where  $\kappa_{*,1}$  and  $\kappa_{*,2}$  are distinct odd primes such that  $\kappa_{*,1} \neq 3$  and  $\kappa_{*,2} \neq 3$ . Thus it follows that  $\left(\frac{\kappa_{*,1}}{\kappa_{*,2}}\right)^{6r}$  is a  $12n$ -th power. Hence there exists a rational number  $\rho \in \mathbb{Q}$  such that

$$\left(\frac{\kappa_{*,1}}{\kappa_{*,2}}\right)^{6r} = (\rho)^{12n}.$$

Applying the  $\kappa_{*,1}$ -adic valuation to both sides of the above identity, we deduce that

$$6r = v_{\kappa_{*,1}} \left( \left( \frac{\kappa_{*,1}}{\kappa_{*,2}} \right)^{6r} \right) = v_{\kappa_{*,1}} ((\rho)^{12n}) = 12n v_{\kappa_{*,1}}(\rho),$$

and hence

$$r = 2n v_{\kappa_{*,1}}(\rho).$$

Thus we deduce that  $n$  divides  $r$ , which is a contradiction since  $1 \leq r \leq m < n$ . Therefore  $\mathcal{D}_{\kappa_1}$  is not isomorphic to  $\mathcal{D}_{\kappa_2}$  for any two distinct integers  $\kappa_1, \kappa_2 \in \mathbf{C}$ . Hence we deduce that  $(\mathcal{D}_\kappa)_{\kappa \in \mathbf{C}}$  is an infinite family of non-isomorphic generalized Mordell curves of degree  $12n$  such that each member in the family  $(\mathcal{D}_\kappa)_{\kappa \in \mathbf{C}}$  is a counterexample to the Hasse principle explained by the Brauer-Manin obstruction. Therefore our contention follows.  $\square$

## 5. THE DESCENDING CHAIN CONDITION ON SEQUENCES OF CURVES

In this section, we will introduce the notion of the *descending chain condition (DCC) on sequences of curves*. This notation provides an analogue of the notion of the descending chain condition on partially ordered sets. Moreover, we will show that the families of generalized Mordell curves constructed in Section 4 satisfy the DCC.

**Definition 5.1.** Let  $(\mathcal{X}_i)_{i \geq 1}$  be a sequence of smooth geometrically irreducible projective curves over a global field  $k$ . For each integer  $i \geq 1$ , let  $\phi_i : \mathcal{X}_{i+1} \rightarrow \mathcal{X}_i$  be a  $k$ -morphism of curves. We say that  $(\mathcal{X}_i, \phi_i)_{i \geq 1}$  satisfies the *descending chain condition (DCC)* if there exists a positive integer  $n$  such that the following are true:

- (DCC1)  $\mathcal{X}_i(k) \neq \emptyset$  for each  $1 \leq i \leq n-1$ .
- (DCC2)  $\mathcal{X}_n$  is a counterexample to the Hasse principle explained by the Brauer-Manin obstruction, i.e.,  $\mathcal{X}_n(\mathbb{A}_k)^{\text{Br}} = \emptyset$  but  $\mathcal{X}_n(\mathbb{A}_k) \neq \emptyset$ .
- (DCC3)  $g_i < g_j$  for any two positive integers  $i, j$  with  $1 \leq i < j$ , where  $g_i$  is the genus of  $\mathcal{X}_i$  for each positive integer  $i$ .

It is not difficult to see that the integer  $n$  in Definition 5.1 is *unique*. When  $n$  satisfies (DCC1)-(DCC3), we define the *length* of  $(\mathcal{X}_i, \phi_i)_{i \geq 1}$  to be  $n$ .

We now explain why Definition 5.1 provides an analogue of the descending chain condition on partially ordered sets. Suppose that  $(\mathcal{X}_i, \phi_i)_{i \geq 1}$  is a sequence of smooth geometrically irreducible projective curves over a global field  $k$ , where the  $\phi_i : \mathcal{X}_{i+1} \rightarrow \mathcal{X}_i$  are  $k$ -morphisms of curves such that  $(\mathcal{X}_i, \phi_i)_{i \geq 1}$  satisfies the DCC in the sense of Definition 5.1. Let  $n$  be the length of  $(\mathcal{X}_i, \phi_i)_{i \geq 1}$ . For  $i = 1$ , set

$$a_1 := \#\mathcal{X}_1(k) \in \mathbb{Z}_{\geq 0} \cup \{\infty\},$$

and for each integer  $i \geq 2$ , define

$$(22) \quad a_i := \#(\phi_1 \circ \phi_2 \circ \cdots \circ \phi_{i-1})(\mathcal{X}_i(k)) \in \mathbb{Z}_{\geq 0} \cup \{\infty\}.$$

The sequence  $(\mathcal{X}_i, \phi_i)_{i \geq 1}$  can be written in the form

$$(23) \quad \cdots \longrightarrow \mathcal{X}_{n+1} \xrightarrow{\phi_n} \mathcal{X}_n \xrightarrow{\phi_{n-1}} \mathcal{X}_{n-1} \xrightarrow{\phi_{n-2}} \cdots \longrightarrow \mathcal{X}_5 \xrightarrow{\phi_4} \mathcal{X}_4 \xrightarrow{\phi_3} \mathcal{X}_3 \xrightarrow{\phi_2} \mathcal{X}_2 \xrightarrow{\phi_1} \mathcal{X}_1.$$

It follows from (22) and (23) that the sequence  $(a_i)_{i \geq 1}$  forms a descending chain of integers, that is, we have that

$$(24) \quad \cdots \leq a_{n+2} \leq a_{n+1} \leq a_n \leq \cdots \leq a_5 \leq a_4 \leq a_3 \leq a_2 \leq a_1.$$

By (DCC2), we know that  $\mathcal{X}_n(\mathbb{A}_k)^{\text{Br}} = \emptyset$ . Since  $\mathcal{X}_n(k) \subseteq \mathcal{X}_n(\mathbb{A}_k)^{\text{Br}}$ , it follows that  $\mathcal{X}_n(k)$  is empty, and hence  $a_n = 0$ . Since  $(\phi_i)_{i \geq 1}$  is a sequence of  $k$ -morphisms of curves and  $\mathcal{X}_n(k) = \emptyset$ , it follows from (23) that  $\mathcal{X}_m(k) = \emptyset$  for each  $m \geq n$ , and thus  $a_m = 0$  for each  $m \geq n$ . By (DCC1), we know that  $a_1 = \#\mathcal{X}_1(k) \geq 1$ . Furthermore, we also know that  $\#\mathcal{X}_i(k) \geq 1$  for each  $2 \leq i \leq n-1$ , and therefore

$$a_i := \#(\phi_1 \circ \phi_2 \circ \cdots \circ \phi_{i-1})(\mathcal{X}_i(k)) \geq 1$$

for each  $2 \leq i \leq n-1$ . Thus we see that the sequence  $(a_i)_{i \geq 1}$  satisfies the descending chain condition in the usual sense; in other words, the descending chain (24) eventually terminates, and satisfies the following two conditions:

- (i)  $1 \leq a_{n-1} \leq a_{n-2} \leq \cdots \leq a_3 \leq a_2 \leq a_1$ , and
- (ii)  $a_m = a_n = 0$  for each  $m \geq n$ .

Note that the descending sequence  $(a_i)_{i \geq 1}$  not only eventually stabilizes but eventually becomes zero.

The above discussion shows that there exists a mapping from the collection of sequences of curves satisfying the DCC in the sense of Definition 5.1 to the collection of descending sequences of integers

satisfying the DCC in the usual sense and eventually becoming zero. More explicitly, we have that

$$\left( \begin{array}{c} \text{sequences of curves } (\mathcal{X}_i, \phi_i)_{i \geq 1} \\ \text{satisfying the DCC} \\ \text{in the sense of Definition 5.1} \end{array} \right) \xrightarrow{\Phi} \left( \begin{array}{c} \text{sequences of integers } (a_i)_{i \geq 1} \\ \text{satisfying the DCC} \\ \text{in the usual sense} \\ \text{and eventually becoming zero} \end{array} \right),$$

where  $\Phi$  is the map sending a sequence  $(\mathcal{X}_i, \phi_i)_{i \geq 1}$  of curves to a sequence  $(a_i)_{i \geq 1}$  of integers defined by

$$a_i := \begin{cases} \#\mathcal{X}_1(k) & \text{if } i = 1, \\ \#(\phi_1 \circ \phi_2 \circ \cdots \circ \phi_{i-1})(\mathcal{X}_i(k)) & \text{if } i \geq 2. \end{cases}$$

**Remark 5.2.** Let  $(\mathcal{X}_i, \phi_i)_{i \geq 1}$  be a sequence of smooth geometrically irreducible curves over a global field  $k$  such that  $(\mathcal{X}_i, \phi_i)_{i \geq 1}$  satisfies the DCC and the length of  $(\mathcal{X}_i, \phi_i)_{i \geq 1}$  is  $n$ . Our main motivation to study the DCC on  $(\mathcal{X}_i, \phi_i)_{i \geq 1}$  is to address the situation where  $\mathcal{X}_n$  has no rational points over  $k$  although it tries hard to possess a  $k$ -rational point. To be more precise, we define

$$\psi_i := \phi_i \circ \phi_{i+1} \circ \cdots \circ \phi_{n-1} : \mathcal{X}_n \longrightarrow \mathcal{X}_i$$

for each  $i \geq 1$ . We see that there are  $n-1$  morphisms  $\psi_i : \mathcal{X}_n \longrightarrow \mathcal{X}_i$  for  $1 \leq i \leq n-1$ . By assumption, we know that  $\#\mathcal{X}_i(k) \geq 1$  for each  $1 \leq i \leq n-1$  and  $\#\mathcal{X}_n(k) = 0$ . For each  $1 \leq i \leq n-1$ , we see that although  $\mathcal{X}_i$  has at least one  $k$ -rational point, there exist no  $k$ -rational points in  $\mathcal{X}_i(k)$  whose preimage under the  $k$ -morphism  $\psi_i$  belongs to  $\mathcal{X}_n(k)$ . Furthermore, by (DDC2), we know that  $\mathcal{X}_n(\mathbb{A}_k) \neq \emptyset$  and  $\mathcal{X}_n(k)$  is a subset of  $\mathcal{X}_n(\mathbb{A}_k)$ . Therefore, although  $\mathcal{X}_n$  tries many ways to obtain at least one  $k$ -rational point, there still exist no  $k$ -rational points on  $\mathcal{X}_n$ .

For each positive integer, it is natural to ask whether there exists a sequence  $(\mathcal{X}_i, \phi_i)_{i \geq 1}$  of curves that satisfies the DCC of length  $n$ . We will answer this question in the affirmative in a stronger form. More precisely, we will prove that for any positive integer  $n$ , there exist infinitely many sequences  $(\mathcal{X}_i, \phi_i)_{i \geq 1}$  of curves that satisfy the DCC of length  $n$ .

**Lemma 5.3.** *Let  $p$  be a prime such that  $p \equiv 1 \pmod{8}$  and  $p \equiv 2 \pmod{3}$ . Let  $n$  and  $m$  be positive integers such that  $2m < n$ . Then there exists an infinite set  $\mathbf{C}_{n,m}$  of integers such that for each integer  $\kappa \in \mathbf{C}_{n,m}$ ,  $\mathcal{D}_{\kappa}^{(m)}$  contains at least two rational points in its affine locus whereas  $\mathcal{D}_{\kappa}^{(n)}$  is a counterexample to the Hasse principle explained by the Brauer-Manin obstruction, where for each  $\kappa \in \mathbf{C}_{n,m}$ ,  $\mathcal{D}_{\kappa}^{(m)}$  and  $\mathcal{D}_{\kappa}^{(n)}$  are the generalized Mordell curves of degree  $12m$  and  $12n$  defined by*

$$(25) \quad \mathcal{D}_{\kappa}^{(m)} : pz^2 = 3^6 \kappa^6 x^{12m} - 1$$

and

$$(26) \quad \mathcal{D}_{\kappa}^{(n)} : pz^2 = 3^6 \kappa^6 x^{12n} - 1,$$

respectively.

*Proof.* Let  $\mathbf{C}_{n,m}$  be the set of nonzero integers  $\kappa$  satisfying the following two conditions:

- (i)  $\kappa = 3^{4m-1} \kappa_*^{2m}$  for some odd prime  $\kappa_* \neq 3$ , and
- (ii)  $\kappa$  satisfies (B3) – (B5) in Section 3 and (C1) – (C3) in Theorem 4.2.

Using Lemma 4.3 with  $(m, r)$  replaced by  $(2m, 2m)$ , we deduce that  $\mathbf{C}_{m,n}$  is of infinite cardinality. Let  $\kappa$  be any nonzero integer in  $\mathbf{C}_{m,n}$ , and let  $\mathcal{D}_{\kappa}^{(m)}$  and  $\mathcal{D}_{\kappa}^{(n)}$  be the smooth projective models defined by (25) and (26), respectively. Since  $\kappa \in \mathbf{C}_{m,n}$ , we know that there exists an odd prime  $\kappa_* \neq 3$  such that  $\kappa = 3^{4m-1} \kappa_*^{2m}$ . The defining equation of  $\mathcal{D}_{\kappa}^{(m)}$  can be written in the form

$$\mathcal{D}_{\kappa}^{(m)} : pz^2 = (3^2 \kappa_* x)^{12m} - 1,$$

and hence we see that the points  $(x, z) = \left( \pm \frac{1}{3^2 \kappa_*}, 0 \right)$  belong to  $\mathcal{D}_{\kappa}^{(m)}(\mathbb{Q})$ . Thus  $\mathcal{D}_{\kappa}^{(m)}$  has at least two  $\mathbb{Q}$ -rational points.

We now prove that  $\mathcal{D}_\kappa^{(n)}$  is a counterexample to the Hasse principle explained by the Brauer-Manin obstruction. Indeed, we know that  $\kappa$  satisfies (B3) – (B5) and (C1) – (C3). By Theorem 4.2, we deduce that  $\mathcal{D}_\kappa^{(n)}$  is a counterexample to the Hasse principle explained by the Brauer-Manin obstruction, and thus our contention follows.  $\square$

**Remark 5.4.** Let  $p$  be a prime such that  $p \equiv 1 \pmod{8}$  and  $p \equiv 2 \pmod{3}$ . Take a positive integer  $n \geq 3$ , and let  $\kappa$  be a nonzero integer. For any positive integer  $s$  dividing  $n$  with  $s \geq 2$ , define  $m_s := \frac{n}{s}$ . Let  $\mathcal{D}_\kappa^{(n)}$  and  $\mathcal{D}_\kappa^{(m_s)}$  be the generalized Mordell curves of degree  $12n$  and  $12m_s$  defined by

$$(27) \quad \mathcal{D}_\kappa^{(n)} : pz^2 = 3^6 \kappa^6 x^{12n} - 1$$

and

$$(28) \quad \mathcal{D}_\kappa^{(m_s)} : pz^2 = 3^6 \kappa^6 x^{12m_s} - 1,$$

respectively. Then there is a  $\mathbb{Q}$ -morphism  $\phi_{m_s} : \mathcal{D}_\kappa^{(n)} \rightarrow \mathcal{D}_\kappa^{(m_s)}$  defined by

$$\begin{aligned} \phi_{m_s} : \mathcal{D}_\kappa^{(n)} &\rightarrow \mathcal{D}_\kappa^{(m_s)} \\ (x, z) &\mapsto (x^s, z). \end{aligned}$$

If  $\kappa$  satisfies (B3) – (B5) and (C1) – (C3) in Theorem 4.2, then we know that  $\mathcal{D}_\kappa^{(n)}$  is a counterexample to the Hasse principle explained by the Brauer-Manin obstruction. Under the morphisms  $\phi_{m_s}$ , it is natural to ask whether one can imply nonexistence of rational points on  $\mathcal{D}_\kappa^{(n)}$  by first showing that there exists a positive integer  $s \geq 2$  such that  $s$  divides  $n$  and the curve  $\mathcal{D}_\kappa^{(m_s)}$  has no rational points, where  $m_s = \frac{n}{s}$ . Lemma 5.3 shows that it is impossible, and thus it proves that the degree  $12n$  of the generalized Mordell curves  $\mathcal{D}$  in Theorem 4.2 is *optimal* in the sense that one can not replace  $n$  by a positive divisor  $m_s$  of  $n$  with  $m_s \neq n$ . Indeed, assume further that  $n$  is odd, and take any positive integer  $s \geq 2$  such that  $s$  divides  $n$ . Define  $m_s := \frac{n}{s}$ . Since  $s \geq 2$ , we deduce that  $2m_s \leq sm_s = n$ . Since  $n$  is odd, we deduce that  $2m_s < n$ . Hence Lemma 5.3 shows that there exists an infinite set  $\mathbf{C}_{n, m_s}$  of integers such that for each  $\kappa \in \mathbf{C}_{n, m_s}$ ,  $\mathcal{D}_\kappa^{(m_s)}$  contains at least two rational points in its affine locus whereas  $\mathcal{D}_\kappa^{(n)}$  is a counterexample to the Hasse principle explained by the Brauer-Manin obstruction, where  $\mathcal{D}_\kappa^{(m_s)}$  and  $\mathcal{D}_\kappa^{(n)}$  are defined by (28) and (27), respectively.

We now prove the main result in this section, which says that for a given positive integer  $h$ , there are infinitely many sequences of curves satisfying the DCC of length  $h$ .

**Corollary 5.5.** *Let  $h$  be a positive integer. Then there are infinitely many sequences  $(\mathcal{X}_i, \phi_i)_{i \geq 1}$  of generalized Mordell curves that satisfy the DCC of length  $h$  in the sense of Definition 5.1, where for each  $i \geq 1$ ,  $\mathcal{X}_i$  is a generalized Mordell curve, and for each  $i \geq 1$ ,*

$$\phi_i : \mathcal{X}_{i+1} \rightarrow \mathcal{X}_i$$

*is a  $k$ -morphism of curves.*

*Proof.* Let  $p$  be a prime such that  $p \equiv 1 \pmod{8}$  and  $p \equiv 2 \pmod{3}$ . Let  $n_0$  and  $n_1$  be integers such that  $n_0 \geq 2$  and  $n_1 \geq 1$ . Set

$$\begin{aligned} n &:= n_0^{h+\epsilon} n_1, \\ m &:= n_0^h n_1, \end{aligned}$$

where  $\epsilon$  is a positive integer such that  $n_0^\epsilon > 2$ . This means that if  $n_0 = 2$ , then  $\epsilon$  is at least two, and that if  $n_0 > 2$ , then  $\epsilon \geq 1$ . We see that

$$2m < mn_0^\epsilon = n.$$

Applying Lemma 5.3 for the triple  $(p, n, m)$ , we deduce that there exists an infinite set  $\mathbf{C}_{n, m}$  of nonzero integers  $\kappa$  satisfying conditions (i) and (ii) as in the proof of Lemma 5.3 such that for any  $\kappa \in \mathbf{C}_{n, m}$ ,

$\mathcal{X}_{h-1}^{(\kappa)}$  contains at least two rational points in its affine locus whereas  $\mathcal{X}_h^{(\kappa)}$  is a counterexample to the Hasse principle explained by the Brauer-Manin obstruction, where for each  $\kappa \in \mathbf{C}_{n,m}$ ,  $\mathcal{X}_{h-1}^{(\kappa)}$  and  $\mathcal{X}_h^{(\kappa)}$  are the generalized Mordell curves defined by

$$\mathcal{X}_{h-1}^{(\kappa)} : pz^2 = 3^6 \kappa^6 x^{12n_0^h n_1} - 1$$

and

$$\mathcal{X}_h^{(\kappa)} : pz^2 = 3^6 \kappa^6 x^{12n_0^{h+\epsilon} n_1} - 1,$$

respectively.

Now take an integer  $\kappa \in \mathbf{C}_{n,m}$ , and let  $\mathcal{X}_{h-1}^{(\kappa)}$  and  $\mathcal{X}_h^{(\kappa)}$  be the smooth projective models as above. Following the proof of Lemma 5.3 and by the definition of  $\mathbf{C}_{n,m}$ , we know that  $\kappa = 3^{4m-1} \kappa_*^{2m}$  for some odd prime  $\kappa_* \neq 3$ . We define

$$\begin{aligned} \psi_{h-1}^{(\kappa)} : \mathcal{X}_h^{(\kappa)} &\rightarrow \mathcal{X}_{h-1}^{(\kappa)} \\ (x, z) &\mapsto (x^{n_0^\epsilon}, z). \end{aligned}$$

For each integer  $i \geq h+1$ , let  $\mathcal{X}_i^{(\kappa)}$  be the smooth projective model of the affine curve defined by

$$\mathcal{X}_i^{(\kappa)} : pz^2 = 3^6 \kappa^6 x^{12n_0^{i+\epsilon} n_1} - 1,$$

and for each integer  $i \geq h$ , let  $\psi_i : \mathcal{X}_{i+1}^{(\kappa)} \rightarrow \mathcal{X}_i^{(\kappa)}$  be the  $\mathbb{Q}$ -morphism of curves defined by

$$\begin{aligned} \psi_i^{(\kappa)} : \mathcal{X}_{i+1}^{(\kappa)} &\rightarrow \mathcal{X}_i^{(\kappa)} \\ (x, z) &\mapsto (x^{n_0}, z). \end{aligned}$$

For each integer  $1 \leq i \leq h-2$ , let  $\mathcal{X}_i^{(\kappa)}$  be the smooth projective model of the affine curve defined by

$$\mathcal{X}_i^{(\kappa)} : pz^2 = 3^6 \kappa^6 x^{12n_0^{i+1} n_1} - 1,$$

and for each integer  $1 \leq i \leq h-2$ , let  $\psi_i : \mathcal{X}_{i+1}^{(\kappa)} \rightarrow \mathcal{X}_i^{(\kappa)}$  be the  $\mathbb{Q}$ -morphism of curves defined by

$$\begin{aligned} \psi_i^{(\kappa)} : \mathcal{X}_{i+1}^{(\kappa)} &\rightarrow \mathcal{X}_i^{(\kappa)} \\ (x, z) &\mapsto (x^{n_0}, z). \end{aligned}$$

Hence we have defined a sequence of curves  $(\mathcal{X}_i^{(\kappa)}, \psi_i^{(\kappa)})_{i \geq 1}$ . We contend that  $(\mathcal{X}_i^{(\kappa)}, \psi_i^{(\kappa)})_{i \geq 1}$  satisfies the DCC of length  $h$  in the sense of Definition 5.1. Indeed, we have shown above that  $\mathcal{X}_h^{(\kappa)}$  is a counterexample to the Hasse principle explained by the Brauer-Manin obstruction, and hence  $(\mathcal{X}_i^{(\kappa)}, \psi_i^{(\kappa)})_{i \geq 1}$  satisfies (DCC2) in Definition 5.1. We also know that  $\mathcal{X}_{h-1}^{(\kappa)}$  contains at least two rational points in its affine locus. Let  $(x_0, z_0)$  be any rational point in  $\mathcal{X}_{h-1}^{(\kappa)}(\mathbb{Q})$ . Then one can check that for each integer  $1 \leq i \leq h-2$ , the point  $(x, z) := (x_0^{n_0^{h-i-1}}, z_0)$  belongs to  $\mathcal{X}_i^{(\kappa)}(\mathbb{Q})$ . Hence (DCC1) is true. It remains to prove that  $(\mathcal{X}_i^{(\kappa)}, \psi_i^{(\kappa)})_{i \geq 1}$  satisfies (DCC3). For each  $i \geq 1$ , we denote by  $g_i^{(\kappa)}$  the genus of the curve  $\mathcal{X}_i^{(\kappa)}$ . We see that

$$g_i^{(\kappa)} = \begin{cases} 6n_0^{i+\epsilon} n_1 - 1 & \text{if } i \geq h, \\ 6n_0^{i+1} n_1 - 1 & \text{if } 1 \leq i \leq h-1. \end{cases}$$

Hence it follows that  $g_i^{(\kappa)} < g_j^{(\kappa)}$  for any positive integers  $i, j$  with  $1 \leq i < j$ , and thus (DCC3) is true. Therefore  $(\mathcal{X}_i^{(\kappa)}, \psi_i^{(\kappa)})_{i \geq 1}$  satisfies the DCC of length  $h$  in the sense of Definition 5.1. Since  $\mathbf{C}_{n,m}$  is of infinite cardinality, our contention follows immediately.  $\square$

The above corollary shows that for a given positive integer  $h \geq 1$ , there are infinitely many sequences of smooth geometrically irreducible curves over  $\mathbb{Q}$  such that they satisfy the DCC of length  $h$ . It is natural to ask whether or not there exists a sequence of smooth geometrically irreducible curves such that it does not satisfy the DCC. The following result shows that there exist infinitely many such sequences of curves over  $\mathbb{Q}$ .

**Proposition 5.6.** *There exist infinitely many sequences of smooth geometrically irreducible curves over  $\mathbb{Q}$  that do not satisfy the DCC in the sense of Definition 5.1.*

*Proof.* Let  $n$  and  $m$  be positive integers such that  $n \geq 2$  and  $m \geq 2$ . Let  $F(x)$  be a separable polynomial of degree  $n$  in  $\mathbb{Q}[x]$  such that  $F(0) \neq 0$  and  $F(1) = 0$ . Note that there are infinitely many such polynomials  $F(x)$ ; for example, one can take  $F(x) = x^n - 1$ . Since  $F(0)$  is nonzero and  $F(x)$  is separable, we see that  $F(x^{m^i})$  is separable for each positive integer  $i \geq 1$ . For each positive integer  $i \geq 1$ , let  $\mathcal{X}_i$  be the smooth projective model of the affine curve defined by

$$\mathcal{X}_i : z^2 = F(x^{m^i}).$$

For each  $i \geq 1$ , we denote by  $g_i$  the genus of  $\mathcal{X}_i$ . For each  $i \geq 1$ , we see that

$$g_i = \begin{cases} \frac{nm^i - 2}{2} & \text{if } nm \equiv 0 \pmod{2}, \\ \frac{nm^i - 1}{2} & \text{if } nm \equiv 1 \pmod{2}. \end{cases}$$

Hence we deduce that  $g_i < g_j$  for any positive integers  $i, j$  with  $1 \leq i < j$ . Since  $F(1) = 0$ , we see that the point  $(x, z) = (1, 0)$  belongs to  $\mathcal{X}_i(\mathbb{Q})$  for each  $i \geq 1$ . Furthermore, for each  $i \geq 1$ , we define

$$\begin{aligned} \psi_i : \mathcal{X}_{i+1} &\longrightarrow \mathcal{X}_i \\ (x, z) &\mapsto (x^m, z). \end{aligned}$$

Hence we have defined a sequence  $(\mathcal{X}_i, \psi_i)_{i \geq 1}$  of smooth geometrically irreducible curves over  $\mathbb{Q}$  such that  $\mathcal{X}_i(\mathbb{Q}) \neq \emptyset$  for each  $i \geq 1$  and  $g_i < g_j$  for any positive integers  $i, j$  with  $1 \leq i < j$ . Thus  $(\mathcal{X}_i, \psi_i)_{i \geq 1}$  does not satisfy the DCC, and therefore our contention follows.  $\square$

## 6. CERTAIN GENERALIZED FERMAT CURVES VIOLATING THE HASSE PRINCIPLE

In this section, we will give a sufficient condition under which certain generalized Fermat curves of signature  $(12n, 12n, 12n)$  with  $n \geq 2$  are counterexamples to the Hasse principle explained by the Brauer-Manin obstruction. In the next section, using this sufficient condition, we will show that for each positive integer  $n \geq 2$ , there exist infinitely many generalized Fermat curves of signature  $(12n, 12n, 12n)$  that are counterexamples to the Hasse principle explained by the Brauer-Manin obstruction. We begin by recalling the following useful result.

**Lemma 6.1.** (see [3, Lemma 4.8])

Let  $k$  be a number field and let  $\mathcal{V}_1$  and  $\mathcal{V}_2$  be (proper)  $k$ -varieties. Assume that there is a  $k$ -morphism  $\Psi : \mathcal{V}_1 \rightarrow \mathcal{V}_2$  and  $\mathcal{V}_2(\mathbb{A}_k)^{\text{Br}} = \emptyset$ . Then  $\mathcal{V}_1(\mathbb{A}_k)^{\text{Br}} = \emptyset$ .

The following theorem is our main result in this section.

**Theorem 6.2.** Let  $p$  be a prime such that  $p \equiv 1 \pmod{8}$  and  $p \equiv 2 \pmod{3}$ . Let  $n$  be an integer such that  $n \geq 2$ , and let  $\chi$  be a nonzero odd integer. Let  $\kappa$  be a nonzero integer satisfying (B3), (B4) and (B5) in Section 3. Assume further that the following are true:

- (D1)  $\kappa \equiv \frac{1}{3} \pmod{p^{2v_p(n)+1}}$ .
- (D2)  $p\chi^2 \equiv 3^6 \kappa^6 \pmod{2^{2v_2(n)+5}}$ .
- (D3)  $p\chi^2 \equiv -1 \pmod{3^{2v_3(n)+3}}$ .
- (D4) let  $\mathbf{D}$  be the set of odd primes  $l$  satisfying the following two conditions:
  - (i)  $\gcd(l, 3) = \gcd(l, p) = 1$ , and



(ii)  $l$  divides  $\kappa$ .

For each prime  $l \in \mathbf{D}$ , we assume that  $l \equiv 1 \pmod{4}$  and  $p\chi^2 \equiv -1 \pmod{l^{2v_l(n)+1}}$ .

(D5) let  $\mathbf{E}$  be the set of odd primes  $l$  satisfying the following two conditions:

- (i)  $\gcd(l, 3) = \gcd(l, p) = \gcd(l, \kappa) = 1$ , and
- (ii)  $l$  divides  $\chi$ .

For each prime  $l \in \mathbf{E}$ , we assume that there exists an integer  $\zeta_l$  with  $\zeta_l \not\equiv 0 \pmod{l}$  such that

$$\kappa \equiv \frac{\zeta_l^{2n}}{3} \pmod{l^{2v_l(n)+1}} \text{ or } \kappa \equiv -\frac{\zeta_l^{2n}}{3} \pmod{l^{2v_l(n)+1}}.$$

(D6) let  $\mathbf{F}$  be the set of odd primes  $l$  satisfying the following two conditions:

- (i)  $\gcd(l, 3) = \gcd(l, p) = \gcd(l, \kappa) = \gcd(l, \chi) = 1$ , and
- (ii)  $l$  divides  $n$ .

For each prime  $l \in \mathbf{F}$ , we assume that  $\kappa \equiv \frac{1}{3} \pmod{l^{2v_l(n)+1}}$ .

(D7) let  $\mathbf{G}$  be the set of odd primes  $l$  satisfying the following two conditions:

- (i)  $\gcd(l, 3) = \gcd(l, p) = \gcd(l, \kappa) = \gcd(l, \chi) = \gcd(l, n) = 1$ , and
- (ii)  $l \leq 4(6n-1)^2(12n-1)^2$ .

For each prime  $l \in \mathbf{G}$ , we assume that  $\kappa \equiv \frac{1}{3} \pmod{l}$ .

Let  $\mathcal{F}$  be the generalized Fermat curve of signature  $(12n, 12n, 12n)$  defined by

$$(29) \quad \mathcal{F} : 3^6 \kappa^6 x^{12n} - y^{12n} - p\chi^2 z^{12n} = 0.$$

Then  $\mathcal{F}$  is a counterexample to the Hasse principle explained by the Brauer-Manin obstruction.

**Remark 6.3.** Let  $\mathcal{F}$  be the generalized Fermat curve of signature  $(12n, 12n, 12n)$  given by (29). It is not difficult to see that the genus of  $\mathcal{F}$  is  $(6n-1)(12n-1)$ .

*Proof.* Let  $\mathcal{D}$  be the smooth projective model in Corollary 3.2 defined by

$$\mathcal{D} : pz^2 = 3^6 \kappa^6 x^{12n} - 1.$$

By Corollary 3.2, we know that  $\mathcal{D}(\mathbb{A}_{\mathbb{Q}})^{\text{Br}} = \emptyset$ . We define

$$\begin{aligned} \Psi : \mathcal{F} &\rightarrow \mathcal{D} \\ (x : y : z) &\mapsto (x : y : \chi z^{6n}). \end{aligned}$$

It is clear that  $\Psi$  is a  $\mathbb{Q}$ -morphism from  $\mathcal{F}$  to  $\mathcal{D}$ . Since  $\mathcal{D}(\mathbb{A}_{\mathbb{Q}})^{\text{Br}} = \emptyset$ , it follows from Lemma 6.1 that  $\mathcal{F}(\mathbb{A}_{\mathbb{Q}})^{\text{Br}} = \emptyset$ . Hence it remains to prove that  $\mathcal{F}$  is everywhere locally solvable.

Note that if  $l$  is an odd prime such that  $l \neq 2, 3, p$  and  $\gcd(l, \kappa\chi n) = 1$ , then  $\mathcal{F}$  is nonsingular modulo  $l$ , and thus the genus of  $\mathcal{F}$  over the finite field  $\mathbb{F}_l$  is  $(6n-1)(12n-1)$ . Hence the Hasse-Weil bound (see Lemma 4.1) assures that  $\mathcal{F}$  is locally solvable at the primes  $l$  such that  $l > 4(6n-1)^2(12n-1)^2$ ,  $l \neq 2, 3, p$  and  $\gcd(l, \kappa\chi n) = 1$ . Hence it suffices to consider the following cases.

★ *Case 1.*  $l = p$ .

We consider the system of equations

$$(30) \quad \begin{cases} G(x, y, z) := 3^6 \kappa^6 x^{12n} - y^{12n} - p\chi^2 z^{12n} &\equiv 0 \pmod{p^{2v_p(n)+1}} \\ \frac{\partial G}{\partial y}(x, y, z) = -12ny^{12n-1} &\equiv 0 \pmod{p^{v_p(n)}} \\ \frac{\partial G}{\partial y}(x, y, z) = -12ny^{12n-1} &\not\equiv 0 \pmod{p^{v_p(n)+1}}. \end{cases}$$

By (D1), we know that

$$G(1, 1, 0) = 3^6 \kappa^6 - 1 \equiv 0 \pmod{p^{2v_p(n)+1}}.$$

Since  $p \neq 2, 3$ , we deduce that

$$\begin{aligned} \frac{\partial G}{\partial y}(1, 1, 0) &= -12n \equiv 0 \pmod{p^{v_p(n)}}, \\ \frac{\partial G}{\partial y}(1, 1, 0) &= -12n \not\equiv 0 \pmod{p^{v_p(n)+1}}. \end{aligned}$$

Hence  $(x, y, z) = (1, 1, 0)$  is a solution to the system (30), and thus it follows from Hensel's lemma that  $\mathcal{F}$  is locally solvable at  $p$ .

★ *Case 2.*  $l = 2$ .

We consider the system of equations

$$(31) \quad \begin{cases} G(x, y, z) := 3^6 \kappa^6 x^{12n} - y^{12n} - p\chi^2 z^{12n} & \equiv 0 \pmod{2^{2v_2(n)+5}} \\ \frac{\partial G}{\partial z}(x, y, z) = -12np\chi^2 z^{12n-1} & \equiv 0 \pmod{2^{v_2(n)+2}} \\ \frac{\partial G}{\partial z}(x, y, z) = -12np\chi^2 z^{12n-1} & \not\equiv 0 \pmod{2^{v_2(n)+3}}. \end{cases}$$

By (D2), we know that

$$G(1, 0, 1) = 3^6 \kappa^6 - p\chi^2 \equiv 0 \pmod{2^{2v_2(n)+5}}.$$

Since  $p \neq 2$  and  $\chi$  is a nonzero odd integer, we see that

$$\begin{aligned} \frac{\partial G}{\partial z}(1, 0, 1) &= -12np\chi^2 = -2^2 \cdot 3np\chi^2 \equiv 0 \pmod{2^{v_2(n)+2}}, \\ \frac{\partial G}{\partial z}(1, 0, 1) &= -12np\chi^2 = -2^2 \cdot 3np\chi^2 \not\equiv 0 \pmod{2^{v_2(n)+3}}. \end{aligned}$$

Hence  $(x, y, z) = (1, 0, 1)$  is a solution to the system (31), and it thus follows from Hensel's lemma that  $\mathcal{F}$  is locally solvable at 2.

★ *Case 3.*  $l = 3$ .

Using the same arguments as in *Case 1* and *Case 2*, it follows from (D3) that  $(x, y, z) = (0, 1, 1)$  is a solution to the system of equations

$$\begin{cases} G(x, y, z) := 3^6 \kappa^6 x^{12n} - y^{12n} - p\chi^2 z^{12n} & \equiv 0 \pmod{3^{2v_3(n)+3}} \\ \frac{\partial G}{\partial y}(x, y, z) = -12ny^{12n-1} & \equiv 0 \pmod{3^{v_3(n)+1}} \\ \frac{\partial G}{\partial y}(x, y, z) = -12ny^{12n-1} & \not\equiv 0 \pmod{3^{v_3(n)+2}}. \end{cases}$$

By Hensel's lemma, we deduce that  $\mathcal{F}$  is locally solvable at 3.

★ *Case 4.*  $l \in \mathbf{D}$ .

Using the same arguments as in *Case 1* and *Case 2*, we deduce from (D4) that  $(x, y, z) = (0, 1, 1)$  is a solution to the system of equations

$$\begin{cases} G(x, y, z) := 3^6 \kappa^6 x^{12n} - y^{12n} - p\chi^2 z^{12n} & \equiv 0 \pmod{l^{2v_l(n)+1}} \\ \frac{\partial G}{\partial y}(x, y, z) = -12ny^{12n-1} & \equiv 0 \pmod{l^{v_l(n)}} \\ \frac{\partial G}{\partial y}(x, y, z) = -12ny^{12n-1} & \not\equiv 0 \pmod{l^{v_l(n)+1}}. \end{cases}$$

By Hensel's lemma, we deduce that  $\mathcal{F}$  is locally solvable at  $l$ .

★ *Case 5.*  $l \in \mathbf{E}$ .

Using the same arguments as in *Case 1* and *Case 2*, we deduce from (D5) that  $(x, y, z) = (1, \zeta_l, 0)$  is a solution to the system of equations

$$\begin{cases} G(x, y, z) := 3^6 \kappa^6 x^{12n} - y^{12n} - p\chi^2 z^{12n} & \equiv 0 \pmod{l^{2v_l(n)+1}} \\ \frac{\partial G}{\partial y}(x, y, z) = -12ny^{12n-1} & \equiv 0 \pmod{l^{v_l(n)}} \\ \frac{\partial G}{\partial y}(x, y, z) = -12ny^{12n-1} & \not\equiv 0 \pmod{l^{v_l(n)+1}}. \end{cases}$$

By Hensel's lemma, we deduce that  $\mathcal{F}$  is locally solvable at  $l$ .

★ *Case 6.*  $l \in \mathbf{F}$ .

Using the same arguments as in *Case 1* and *Case 2*, we deduce from (D6) that  $(x, y, z) = (1, 1, 0)$  is a solution to the system of equations

$$\begin{cases} G(x, y, z) := 3^6 \kappa^6 x^{12n} - y^{12n} - p\chi^2 z^{12n} & \equiv 0 \pmod{l^{2v_l(n)+1}} \\ \frac{\partial G}{\partial y}(x, y, z) = -12ny^{12n-1} & \equiv 0 \pmod{l^{v_l(n)}} \\ \frac{\partial G}{\partial y}(x, y, z) = -12ny^{12n-1} & \not\equiv 0 \pmod{l^{v_l(n)+1}}. \end{cases}$$

By Hensel's lemma, we deduce that  $\mathcal{F}$  is locally solvable at  $l$ .

★ *Case 7.*  $l \in \mathbf{G}$ .

Using the same arguments as in *Case 1* and *Case 2*, we deduce from (D7) that  $(x, y, z) = (1, 1, 0)$  is a solution to the system of equations

$$\begin{cases} G(x, y, z) := 3^6 \kappa^6 x^{12n} - y^{12n} - p\chi^2 z^{12n} & \equiv 0 \pmod{l} \\ \frac{\partial G}{\partial y}(x, y, z) = -12ny^{12n-1} & \not\equiv 0 \pmod{l}. \end{cases}$$

By Hensel's lemma, we deduce that  $\mathcal{F}$  is locally solvable at  $l$ .

★ *Case 8.*  $l = \infty$ .

We see that the point  $(x, y, z) = (1, (3^6 \kappa^6)^{1/12n}, 0)$  belongs to  $\mathcal{F}(\mathbb{R})$ .

Thus, by what we have shown,  $\mathcal{F}$  is everywhere locally solvable, and therefore our contention follows.  $\square$

## 7. INFINITUDE OF THE QUADRUPLES $(p, n, \kappa, \chi)$

In this section, we will prove that there are infinitely many couples  $(\kappa, \chi)$  satisfying (D1) – (D7) in Theorem 6.2. Hence this implies that for each integer  $n \geq 2$ , there exist infinitely many generalized Fermat curves of signature  $(12n, 12n, 12n)$  that are counterexamples to the Hasse principle explained by the Brauer-Manin obstruction. We begin by proving some elementary but very useful lemmas that we will need in the proof of the main result of this section.

**Lemma 7.1.** *Let  $s$  be a positive odd integer. Let  $(P, Q, R, S)$  be a quadruple of integers such that  $R \neq 0$ . Assume that the following are true:*

- (i)  $sP \equiv 1 \pmod{R}$  and  $Q = 1 + \frac{sP-1}{R}$ .
- (ii)  $q := sS + Q$  is an odd prime.

*Then every integer is an  $s$ -th power in  $\mathbb{Z}/q\mathbb{Z}$ .*

*Proof.* Let  $h$  be an integer. If  $h \equiv 0 \pmod{q}$ , then  $h$  is an  $s$ -th power in  $\mathbb{Z}/q\mathbb{Z}$ . If  $h \not\equiv 0 \pmod{q}$ , then we see that

$$(h^{RS+P})^s = h^{sRS+sP} = h^{sS+Q} h^{(R-1)(sS+Q-1)} = h^q h^{(R-1)(q-1)} \equiv h \pmod{q}.$$

Therefore  $h$  is an  $s$ -th power in  $\mathbb{Z}/q\mathbb{Z}$ , which proves our contention.  $\square$

**Lemma 7.2.** *Let  $s$  be a positive odd integer, and let  $r$  be an integer such that  $\gcd(r-1, s) = 1$ . Let  $S$  be an integer, and define  $q := sS + r$ . Assume that  $q$  is an odd prime. Then every integer is an  $s$ -th power in  $\mathbb{Z}/q\mathbb{Z}$ .*

*Proof.* We show that there is a triple  $(P, Q, R)$  of integers with  $R \neq 0$  such that the quintuple  $(q, P, Q, R, S)$  satisfies conditions (i) and (ii) in Lemma 7.1. Indeed, since  $\gcd(r-1, s) = 1$ , there exist nonzero integers  $P, R$  such that

$$sP + (1-r)R = 1.$$

Hence we deduce that

$$sP - 1 = R(r-1),$$

and thus  $sP \equiv 1 \pmod{R}$ . Define

$$Q := 1 + \frac{sP-1}{R}.$$

Since  $R$  divides  $sP - 1$ , we know that  $Q$  is an integer. Since  $sP - 1 = R(r-1)$ , we deduce that

$$Q = 1 + \frac{sP-1}{R} = 1 + r - 1 = r,$$

and hence  $q = sS + r = sS + Q$ . Thus it follows from Lemma 7.1 that every integer is an  $s$ -th power in  $\mathbb{Z}/q\mathbb{Z}$ .  $\square$

**Lemma 7.3.** *Let  $l$  be an odd prime, and let  $r$  be an integer such that  $\gcd(r, l) = 1$ . Then at least one of the integers  $r - 1$  and  $-r - 1$  is relatively prime to  $l$ .*

*Proof.* Assume the contrary, that is,  $r - 1 \equiv 0 \pmod{l}$  and  $-r - 1 \equiv 0 \pmod{l}$ . Hence we deduce that

$$-2 \equiv (r - 1) + (-r - 1) \equiv 0 \pmod{l},$$

which is a contradiction since  $l$  is an odd prime. Thus our contention follows.  $\square$

**Lemma 7.4.** *Let  $l$  be an odd prime such that  $l \equiv 3 \pmod{4}$ . Let  $x$  be an integer such that  $x$  is a square in  $\mathbb{F}_l^\times$ . Then, for any positive integer  $n$ ,  $x$  is a  $2^n$ -th power in  $\mathbb{F}_l^\times$ , that is, there exists an integer  $x_*$  such that  $x_* \not\equiv 0 \pmod{l}$  and  $x_*^{2^n} \equiv x \pmod{l}$ .*

*Proof.* We prove Lemma 7.4 by induction over  $n$ .

If  $n = 1$ , then it follows immediately from the assumption that  $x$  is a square in  $\mathbb{F}_l^\times$ . Assume that Lemma 7.4 is true for  $n - 1$  with  $n \geq 2$ . We will prove that it is also true for  $n$ . Indeed, by the induction hypothesis, we know that there is an integer  $h$  such that  $h^{2^{n-1}} \equiv x \pmod{l}$ . Since  $x$  belongs to  $\mathbb{F}_l^\times$ , the last congruence implies that  $h$  belongs to  $\mathbb{F}_l^\times$ . If  $h$  is a square in  $\mathbb{F}_l^\times$ , then it follows that  $x_*^{2^n} \equiv x \pmod{l}$ , where  $x_*$  is an integer such that  $x_*^2 \equiv h \pmod{l}$ . Assume now that  $h$  is not a square in  $\mathbb{F}_l^\times$ , that is,  $\left(\frac{h}{l}\right) = -1$ , where  $\left(\frac{\cdot}{\cdot}\right)$  denotes the Jacobi symbol. Since  $l \equiv 3 \pmod{4}$ , we know that  $\left(\frac{-1}{l}\right) = -1$ , and hence it follows that

$$\left(\frac{-h}{l}\right) = \left(\frac{h}{l}\right) \left(\frac{-1}{l}\right) = 1.$$

Thus there is an integer  $x_*$  such that  $x_*^2 \equiv -h \pmod{l}$ . Therefore we deduce that

$$x_*^{2^n} = (x_*^2)^{2^{n-1}} \equiv (-h)^{2^{n-1}} \equiv (-1)^{2^{n-1}} h^{2^{n-1}} \equiv x \pmod{l},$$

which proves our contention.  $\square$

**Lemma 7.5.** *Let  $p$  be a prime such that  $p \equiv 1 \pmod{8}$  and  $p \equiv 2 \pmod{3}$ . Let  $n$  and  $m$  be positive integers such that  $n \geq 2$  and  $1 \leq m < n$ . Then, for any positive integer  $r$  dividing  $m$ , there are infinitely many couples  $(\kappa, \chi)$  of integers such that the following are true:*

- (i)  $\kappa$  satisfies (B3) – (B5) in Section 3.
- (ii)  $\kappa = 3^{2^{m-1}} \kappa_*^r$  for some odd prime  $\kappa_*$  with  $\kappa_* \neq 3$ .
- (iii)  $\chi$  is an odd prime.
- (iv)  $(p, n, \kappa, \chi)$  satisfies (D1) – (D7) in Theorem 6.2.

*Proof.* Let  $r$  be a positive integer such that  $r$  divides  $m$ , and define

$$s := \frac{m}{r}.$$

Let  $\mathbf{F}^*$  be the set of odd primes  $l$  satisfying the following two conditions:

- (i)  $\gcd(l, 3) = \gcd(l, p) = 1$ , and
- (ii)  $l$  divides  $n$ .

Let  $\mathbf{G}^*$  be the set of odd primes  $l$  satisfying the following two conditions:

- (i)  $\gcd(l, 3) = \gcd(l, p) = \gcd(l, n) = 1$ , and
- (ii)  $l \leq 4(6n - 1)^2(12n - 1)^2$ .

★ *Step 1. Choosing  $\kappa$ .*

Note that 2, 3 and  $p$  do not belong to  $\mathbf{F}^*$  and  $\mathbf{G}^*$ , and that  $\mathbf{F}^* \cap \mathbf{G}^* = \emptyset$ . Hence, by the Chinese Remainder Theorem, there exists an integer  $\kappa_{*,0}$  such that the following are true:

$$(E1) \quad \kappa_{*,0} \equiv 1 \pmod{4},$$

$$\begin{aligned}
(E2) \quad \kappa_{*,0} &\equiv \frac{1}{3^{2s}} \pmod{p^{2v_p(n)+1}}, \\
(E3) \quad \kappa_{*,0} &\equiv \frac{1}{3^{2s}} \pmod{l^{2v_l(n)+1}} \text{ for each } l \in \mathbf{F}^*, \text{ and} \\
(E4) \quad \kappa_{*,0} &\equiv \frac{1}{3^{2s}} \pmod{l} \text{ for each } l \in \mathbf{G}^*.
\end{aligned}$$

Let  $Q(X) \in \mathbb{Z}[X]$  be the linear polynomial defined by

$$(32) \quad Q(X) := 2^2 \cdot p^{2v_p(n)+1} \left( \prod_{l \in \mathbf{F}^*} l^{2v_l(n)+1} \right) \left( \prod_{l \in \mathbf{G}^*} l \right) X + \kappa_{*,0}.$$

By (E1), (E2), (E3) and (E4) above, we know that

$$\gcd \left( \kappa_{*,0}, 2^2 \cdot p^{2v_p(n)+1} \left( \prod_{l \in \mathbf{F}^*} l^{2v_l(n)+1} \right) \left( \prod_{l \in \mathbf{G}^*} l \right) \right) = 1.$$

Applying Dirichlet's theorem on arithmetic progressions, we deduce that there are infinitely many integers  $X$  such that  $Q(X) \neq 3$ ,  $Q(X) \neq p$  and  $Q(X)$  is an odd prime. Take such an integer  $X$ , and set

$$\kappa_* := Q(X).$$

Define

$$(33) \quad \kappa := 3^{2m-1} \kappa_*^r.$$

★ *Step 2. Choosing  $\chi_*$ .*

By (32) and (E2), we see that

$$\kappa_* \equiv \kappa_{*,0} \equiv \frac{1}{3^{2s}} \pmod{p^{2v_p(n)+1}}.$$

This implies that  $\kappa_* \equiv \frac{1}{3^{2s}} \pmod{p}$ , and hence it follows that  $\left( \frac{\kappa_*}{p} \right) = 1$ , where  $\left( \frac{\cdot}{\cdot} \right)$  denotes the Jacobi symbol. Since  $\kappa_*$  is an odd prime and  $p \equiv 1 \pmod{8}$ , it follows from the quadratic reciprocity law that

$$\left( \frac{p}{\kappa_*} \right) = 1.$$

By (32) and (E1), we deduce that  $\kappa_* \equiv \kappa_{*,0} \equiv 1 \pmod{4}$ . Hence  $-1$  is a square in the finite field  $\mathbb{F}_{\kappa_*}$ , and thus it follows that

$$\left( \frac{-p}{\kappa_*} \right) = \left( \frac{-1}{\kappa_*} \right) \left( \frac{p}{\kappa_*} \right) = 1.$$

Therefore  $-\frac{1}{p}$  is a square in  $\mathbb{Z}_{\kappa_*}^\times$ , and hence there exist an element  $\Gamma_{\kappa_*}$  in  $\mathbb{Z}_{\kappa_*}^\times$  and an integer  $\Gamma_{\kappa_*,0}$  such that

$$(34) \quad \begin{cases} \Gamma_{\kappa_*}^2 &= -\frac{1}{p} \\ \Gamma_{\kappa_*} &\equiv \Gamma_{\kappa_*,0} \pmod{\kappa_*^{2v_{\kappa_*}(n)+1}}. \end{cases}$$

By assumption, we know that  $-p \equiv -2 \equiv 1 \pmod{3}$ , and hence we deduce that  $-\frac{1}{p}$  is a square in  $\mathbb{Z}_3^\times$ . Thus there exist an element  $\Gamma_3$  in  $\mathbb{Z}_3^\times$  and an integer  $\Gamma_{3,0}$  such that

$$(35) \quad \begin{cases} \Gamma_3^2 &= -\frac{1}{p} \\ \Gamma_3 &\equiv \Gamma_{3,0} \pmod{3^{2v_3(n)+3}}. \end{cases}$$

By assumption, we know that  $p \equiv 1 \pmod{8}$ , and hence we deduce that  $\frac{1}{p}$  is a square in  $\mathbb{Z}_2^\times$ . Thus there exist an element  $\Gamma_2$  in  $\mathbb{Z}_2^\times$  and an integer  $\Gamma_{2,0}$  such that

$$(36) \quad \begin{cases} \Gamma_2^2 &= \frac{1}{p} \\ \Gamma_2 &\equiv \Gamma_{2,0} \pmod{2^{2v_2(n)+5}}. \end{cases}$$

Let  $\Delta_2, \Delta_3$  and  $\Delta_{\kappa_*}$  be integers in  $\{\pm 1\}$ , which will be determined later. Let  $\mathbf{H}$  be the set of odd primes  $l$  satisfying the following two conditions:

- (i)  $\gcd(l, 3) = \gcd(l, \kappa_*) = 1$ , and
- (ii)  $l$  divides  $n$ .

Since  $\kappa_* \neq 2, 3$  and  $\mathbf{H}$  does not contain  $2, 3$  and  $\kappa_*$ , it follows from the Chinese remainder theorem that there exists an integer  $\chi_*$  such that the following are true:

- (E5)  $\chi_* \equiv \Theta_2 \pmod{2^{2v_2(n)+5}}$ ,
- (E6)  $\chi_* \equiv \Theta_3 \pmod{3^{2v_3(n)+3}}$ ,
- (E7)  $\chi_* \equiv \Theta_{\kappa_*} \pmod{\kappa_*^{2v_{\kappa_*}(n)+1}}$ , and
- (E8)  $\chi_* \equiv \Theta_l \pmod{l^{v_l(n)}}$  for each prime  $l \in \mathbf{H}$ .

Here

$$(37) \quad \begin{cases} \Theta_2 &:= \Delta_2 \Gamma_{2,0} 3^3 \kappa^3 \\ \Theta_3 &:= \Delta_3 \Gamma_{3,0} \\ \Theta_{\kappa_*} &:= \Delta_{\kappa_*} \Gamma_{\kappa_*,0}, \end{cases}$$

and for each prime  $l \in \mathbf{H}$ , take  $\Theta_l$  to be an integer such that

$$(38) \quad \gcd(\Theta_l, l) = \gcd(\Theta_l - 1, l) = 1.$$

Note that for each prime  $l \in \mathbf{H}$ , there exist infinitely many integers  $\Theta_l$  satisfying (38); for example, one can take  $\Theta_l$  to be any integer such that  $\Theta_l \equiv 2 \pmod{l}$  for each prime  $l \in \mathbf{H}$ .

★ *Step 3. Choosing  $\Delta_2, \Delta_3$  and  $\Delta_{\kappa_*}$ .*

We first choose  $\Delta_2$ . Since  $\Gamma_{2,0}^2 \equiv \Gamma_2^2 = \frac{1}{p} \pmod{2^{2v_2(n)+5}}$ , it follows that  $\Gamma_{2,0}$  is odd, and hence either  $\Gamma_{2,0} \equiv 1 \pmod{4}$  or  $\Gamma_{2,0} \equiv -1 \pmod{4}$ . By (32), (33) and (E1), we see that

$$3^3 \kappa^3 = 3^3 (3^{2m-1} \kappa_*^r)^3 \equiv (-1)^3 (-1)^{3(2m-1)} \kappa_{*,0}^{3r} \equiv 1 \pmod{4}.$$

Thus we deduce that either  $\Gamma_{2,0} 3^3 \kappa^3 \equiv 1 \pmod{4}$  or  $\Gamma_{2,0} 3^3 \kappa^3 \equiv -1 \pmod{4}$ . We choose  $\Delta_2 \in \{\pm 1\}$  such that

$$(39) \quad \Theta_2 = \Delta_2 \Gamma_{2,0} 3^3 \kappa^3 \equiv -1 \equiv 3 \pmod{4}.$$

We now choose  $\Delta_3$ . Since  $\Gamma_{3,0}^2 \equiv \Gamma_3^2 = -\frac{1}{p} \pmod{3^{2v_3(n)+3}}$  and  $-p \equiv -2 \equiv 1 \pmod{3}$ , it follows that  $\Gamma_{3,0}^2 \equiv -\frac{1}{p} \equiv 1 \pmod{3}$ , and hence either  $\Gamma_{3,0} \equiv 1 \pmod{3}$  or  $\Gamma_{3,0} \equiv -1 \pmod{3}$ . We choose  $\Delta_3 \in \{\pm 1\}$  such that

$$(40) \quad \Theta_3 = \Delta_3 \Gamma_{3,0} \equiv -1 \equiv 2 \pmod{3}.$$

We now define  $\Delta_{\kappa_*}$ . By (34), we know that  $\Gamma_{\kappa_*,0} \not\equiv 0 \pmod{\kappa_*}$ , and hence  $\gcd(\Gamma_{\kappa_*,0}, \kappa_*) = 1$ . Using Lemma 7.3 with  $(r, l)$  replaced by  $(\Gamma_{\kappa_*,0}, \kappa_*)$ , we deduce that there is a choice of  $\Delta_{\kappa_*} \in \{\pm 1\}$  such that

$$(41) \quad \gcd(\Theta_{\kappa_*} - 1, \kappa_*) = \gcd(\Delta_{\kappa_*} \Gamma_{\kappa_*,0} - 1, \kappa_*) = 1.$$

★ *Step 4. Choosing  $\chi$ .*

Define

$$(42) \quad \Upsilon := 2^{2v_2(n)+5} \cdot 3^{2v_3(n)+3} \cdot \kappa_*^{2v_{\kappa_*}(n)+1} \prod_{l \in \mathbf{H}} l^{v_l(n)},$$

where  $\mathbf{H}$  was defined in *Step 2*. Let  $R(Y) \in \mathbb{Z}[Y]$  be the linear polynomial defined by

$$(43) \quad R(Y) := \Upsilon Y + \chi_*,$$

where  $\chi_*$  was chosen in *Step 2*. By (E5), (E6), (E7) and (E8), we see that

$$\gcd(\chi_*, \Upsilon) = 1.$$

By Dirichlet's theorem on arithmetic progressions, we deduce that there are infinitely many integers  $Y$  such that  $R(Y)$  is an odd prime. Take such an integer  $Y$ , and define

$$(44) \quad \chi := R(Y).$$

Set

$$(45) \quad n_* := \frac{n}{2^{v_2(n)}} \in \mathbb{Z}.$$

By (42) and noting that  $n_*$  can be written in the form

$$n_* = \frac{n}{2^{v_2(n)}} = 3^{v_3(n)} \kappa_*^{v_{\kappa_*}(n)} \prod_{l \in \mathbf{H}} l^{v_l(n)},$$

we see that  $\Upsilon$  can be written in the form

$$\Upsilon = \left( 2^{2v_2(n)+5} \cdot 3^{v_3(n)+3} \cdot \kappa_*^{v_{\kappa_*}(n)+1} \right) n_*.$$

Hence we deduce that

$$\chi = R(Y) = \Upsilon Y + \chi_* = \left( 2^{2v_2(n)+5} \cdot 3^{v_3(n)+3} \cdot \kappa_*^{v_{\kappa_*}(n)+1} \right) n_* Y + \chi_*,$$

and thus we have that

$$(46) \quad \chi = n_* \Sigma_{n_*} + \chi_*,$$

where

$$\Sigma_{n_*} := \left( 2^{2v_2(n)+5} \cdot 3^{v_3(n)+3} \cdot \kappa_*^{v_{\kappa_*}(n)+1} \right) Y.$$

*★ Step 5. Verifying (B3) – (B5) in Section 3 and (D1) – (D7) in Theorem 6.2.*

We first verify (B3) – (B5) in Section 3. Recall that  $\kappa_*$  is an odd prime such that  $\kappa_* \neq 3$ . Hence it follows from (33) that

$$v_3(\kappa) = v_3(3^{2m-1} \kappa_*^r) = 2m - 1 < 2n - 1,$$

which proves that (B3) is true. In *Step 1*, we have chosen  $\kappa_*$  to be an odd prime such that  $\kappa_* \neq p$ . Since  $\kappa = 3^{2m-1} \kappa_*^r \not\equiv 0 \pmod{p}$ , we deduce that (B4) holds.

We now prove that (B5) holds. Indeed, let  $l$  be any odd prime such that  $\gcd(l, 3) = 1$  and  $l$  divides  $\kappa$ . By (33), we deduce that  $l = \kappa_*$ . By (32) and (E2), we know that

$$\kappa_* = Q(X) \equiv \kappa_{*,0} \equiv \frac{1}{3^{2s}} \pmod{p^{2v_p(n)+1}}.$$

This implies that  $\kappa_* \equiv \frac{1}{3^{2s}} \pmod{p}$ , and thus  $\left( \frac{\kappa_*}{p} \right) = 1$ . Since  $p \equiv 1 \pmod{8}$ , it follows from the quadratic reciprocity law that  $\left( \frac{p}{\kappa_*} \right) = 1$ . In other words,  $p$  is a square in  $\mathbb{Q}_{\kappa_*}^\times$ , and hence (B5) is true.

We now verify (D1) – (D7) in Theorem 6.2. Let  $\mathbf{D}, \mathbf{E}, \mathbf{F}$  and  $\mathbf{G}$  the sets of odd primes that were defined in Theorem 6.2. It is not difficult to see that (D1), (D6) and (D7) are true. Indeed, we see that  $\mathbf{F} \subseteq \mathbf{F}^*$  and  $\mathbf{G} \subseteq \mathbf{G}^*$ , where the sets  $\mathbf{F}^*$  and  $\mathbf{G}^*$  were defined in the paragraph preceding *Step 1*.



For any odd prime  $l \in \mathbf{F}^*$ , it follows from (E3), (32) and (33) that

$$\begin{aligned}\kappa &= 3^{2m-1}\kappa_*^r = 3^{2m-1}Q(X)^r \equiv 3^{2m-1}\kappa_{*,0}^r \equiv 3^{2m-1}\frac{1}{3^{2rs}} \\ &\equiv 3^{2m-1}\frac{1}{3^{2m}} \quad (\text{since } rs = m) \\ &\equiv \frac{1}{3} \quad (\text{mod } l^{2v_l(n)+1}).\end{aligned}$$

Since  $\mathbf{F} \subseteq \mathbf{F}^*$ , we deduce that  $\kappa \equiv \frac{1}{3} \pmod{l^{2v_l(n)+1}}$  for any  $l \in \mathbf{F}^*$ , and thus (D6) is true. Using the same arguments, one can show that (D1) and (D7) are true.

We now prove that (D2), (D3) and (D4) hold. By (36), (E5), (37), (42), (43) and (44), we see that

$$\begin{aligned}p\chi^2 &= pR(Y)^2 \equiv p\chi_*^2 \equiv p\Theta_2^2 \equiv p\Delta_2^2\Gamma_{2,0}^2 3^6 \kappa^6 \\ &\equiv p\Gamma_2^2 3^6 \kappa^6 \quad (\text{since } \Delta_2^2 = 1) \\ &\equiv p\frac{1}{p} 3^6 \kappa^6 \quad (\text{by (36)}) \\ &\equiv 3^6 \kappa^6 \quad (\text{mod } 2^{2v_2(n)+5}),\end{aligned}$$

and hence (D2) is true.

By (35), (E6), (37), (42), (43) and (44), we see that

$$\begin{aligned}p\chi^2 &= pR(Y)^2 \equiv p\chi_*^2 \equiv p\Theta_3^2 \equiv p\Delta_3^2\Gamma_{3,0}^2 \\ &\equiv p\Gamma_3^2 \quad (\text{since } \Delta_3^2 = 1) \\ &\equiv p\left(-\frac{1}{p}\right) \quad (\text{by (35)}) \\ &\equiv -1 \quad (\text{mod } 3^{2v_3(n)+3}),\end{aligned}$$

and hence (D3) is true.

We now show that (D4) holds. By (33) and since  $\kappa_*$  is an odd prime such that  $\kappa_* \neq 3$  and  $\kappa_* \neq p$ , we see that  $\mathbf{D} = \{\kappa_*\}$ , where  $\mathbf{D}$  is the set of odd primes that was defined in Theorem 6.2. By (E1) and (32), we know that

$$\kappa_* = Q(X) \equiv \kappa_{*,0} \equiv 1 \pmod{4}.$$

By (34), (E7), (37), (42), (43) and (44), we see that

$$\begin{aligned}p\chi^2 &= pR(Y)^2 \equiv p\chi_*^2 \equiv p\Theta_{\kappa_*}^2 \equiv p\Delta_{\kappa_*}^2\Gamma_{\kappa_*,0}^2 \\ &\equiv p\Gamma_{\kappa_*}^2 \quad (\text{since } \Delta_{\kappa_*}^2 = 1) \\ &\equiv p\left(-\frac{1}{p}\right) \quad (\text{by (34)}) \\ &\equiv -1 \quad (\text{mod } \kappa_*^{2v_{\kappa_*}(n)+1}),\end{aligned}$$

and hence (D4) is true.

Finally, we prove that (D5) holds. Since  $\chi$  is an odd prime, we deduce that either  $\mathbf{E} = \emptyset$  or  $\mathbf{E} = \{\chi\}$ . By (E5), (E6), (E7), (E8) and (44), we deduce that

$$(47) \quad \chi \equiv \chi_* \not\equiv 0 \pmod{2},$$

$$(48) \quad \chi \equiv \chi_* \not\equiv 0 \pmod{3},$$

$$(49) \quad \chi \equiv \chi_* \not\equiv 0 \pmod{\kappa_*}.$$

By (E8) and (38), we know that

$$(50) \quad \chi \equiv \chi_* \equiv \Theta_l \not\equiv 0 \pmod{l}$$

for every odd prime  $l \in \mathbf{H}$ . Since

$$n = 2^{v_2(n)} \cdot 3^{v_3(n)} \cdot \kappa_*^{v_{\kappa_*}(n)} \prod_{l \in \mathbf{H}} l^{v_l(n)},$$

it follows from the last congruences that  $\gcd(\chi, n) = 1$ , and thus  $v_\chi(n) = 0$ . Hence we see that in order to prove that (D5) holds, it suffices to prove that there exists an integer  $\zeta_\chi$  with  $\zeta_\chi \not\equiv 0 \pmod{\chi}$  such that either  $\kappa \equiv \frac{\zeta_\chi^{2n}}{3} \pmod{\chi}$  or  $\kappa \equiv -\frac{\zeta_\chi^{2n}}{3} \pmod{\chi}$ .

By (33) and since  $\chi \not\equiv 0 \pmod{3}$  and  $\chi \not\equiv 0 \pmod{\kappa_*}$ , we see that  $\gcd(\chi, 3\kappa) = 1$ . By (E5), (39) and (44), we deduce that

$$\chi = R(Y) \equiv \chi_* \equiv \Theta_2 \equiv 3 \pmod{4}.$$

We contend that there is an integer  $\rho \in \{\pm 1\}$  such that  $\rho 3\kappa$  is a square in  $\mathbb{F}_\chi^\times$ . Indeed, if  $3\kappa$  is a square in  $\mathbb{F}_\chi^\times$ , then we let  $\rho = 1$ . Assume that  $3\kappa$  is not a square in  $\mathbb{F}_\chi^\times$ , i.e.,  $\left(\frac{3\kappa}{\chi}\right) = -1$ . Since  $\chi \equiv 3 \pmod{4}$ , we know that  $-1$  is a quadratic non-residue in  $\mathbb{F}_\chi^\times$ . Hence it follows that

$$\left(\frac{-3\kappa}{\chi}\right) = \left(\frac{3\kappa}{\chi}\right) \left(\frac{-1}{\chi}\right) = 1,$$

which proves that  $\rho 3\kappa$  is a square in  $\mathbb{F}_\chi^\times$ , where  $\rho = -1$ . For the rest of the proof, fix an integer  $\rho \in \{\pm 1\}$  such that  $\rho 3\kappa$  is a square in  $\mathbb{F}_\chi^\times$ .

Since  $\chi \equiv 3 \pmod{4}$ , using Lemma 7.4 with  $(l, x)$  replaced by  $(\chi, \rho 3\kappa)$ , we deduce that  $\rho 3\kappa$  is a  $2^{v_2(n)+1}$ -th power in  $\mathbb{F}_\chi^\times$ . In other words, there is an integer  $\tau$  such that  $\tau \not\equiv 0 \pmod{\chi}$  and

$$(51) \quad \tau^{2^{v_2(n)+1}} \equiv \rho 3\kappa \pmod{\chi}.$$

We prove that  $\gcd(\chi_* - 1, n_*) = 1$ , where  $n_*$  is defined by (45). Indeed, by (E6) and (40), we know that

$$(52) \quad \chi_* - 1 \equiv \Theta_3 - 1 \equiv 1 \pmod{3}.$$

By (E7) and (41), we see that

$$(53) \quad \chi_* - 1 \equiv \Theta_{\kappa_*} - 1 \not\equiv 0 \pmod{\kappa_*}.$$

Recall from (E8) and (38) that for each prime  $l \in \mathbf{H}$ , we have that

$$(54) \quad \chi_* - 1 \equiv \Theta_l - 1 \not\equiv 0 \pmod{l}.$$

Since

$$n_* = \frac{n}{2^{v_2(n)}} = 3^{v_3(n)} \cdot \kappa_*^{v_{\kappa_*}(n)} \prod_{l \in \mathbf{H}} l^{v_l(n)},$$

it follows from (52), (53) and (54) that

$$\gcd(\chi_* - 1, n_*) = 1.$$

By (47), (48), (49) and (50) and since

$$n_* = \frac{n}{2^{v_2(n)}} = 3^{v_3(n)} \cdot \kappa_*^{v_{\kappa_*}(n)} \prod_{l \in \mathbf{H}} l^{v_l(n)},$$

we see that  $\gcd(\chi_*, n_*) = 1$ , and hence it follows that

$$\gcd(\chi_*, n_*) = 1 = \gcd(\chi_* - 1, n_*).$$

We recall from (46) that

$$\chi = n_* \Sigma_{n_*} + \chi_*.$$

Hence, using Lemma 7.2 with  $(r, s, q, S)$  replaced by  $(\chi_*, n_*, \chi, \Sigma_{n_*})$ , we deduce that every integer is an  $n_*$ -th power in  $\mathbb{F}_\chi$ . Since  $\tau \not\equiv 0 \pmod{\chi}$ , this implies that  $\tau$  is an  $n_*$ -th power in  $\mathbb{F}_\chi^\times$ . In other words, there exists an integer  $\zeta_\chi$  such that  $\zeta_\chi \not\equiv 0 \pmod{\chi}$  and

$$(55) \quad \tau \equiv \zeta_\chi^{n_*} \pmod{\chi}.$$

By (51), (55) and since  $n = 2^{v_2(n)} n_*$ , we deduce that

$$\begin{aligned} \rho 3\kappa &\equiv \tau^{2^{v_2(n)+1}} \equiv (\zeta_\chi^{n_*})^{2^{v_2(n)+1}} \\ &\equiv (\zeta_\chi)^{n_* 2^{v_2(n)+1}} \\ &\equiv \zeta_\chi^{2n} \pmod{\chi}. \end{aligned}$$

Since either  $\rho = 1$  or  $\rho = -1$ , we see that  $\rho^2 = 1$ , and hence it follows that

$$\kappa \equiv \frac{\zeta_\chi^{2n}}{3\rho} \equiv \rho \frac{\zeta_\chi^{2n}}{3\rho^2} \equiv \rho \frac{\zeta_\chi^{2n}}{3} \pmod{\chi},$$

which proves that (D5) holds. Hence our contention follows.  $\square$

**Corollary 7.6.** *Let  $p$  be a prime such that  $p \equiv 1 \pmod{8}$  and  $p \equiv 2 \pmod{3}$ . Let  $n$  and  $m$  be positive integers such that  $n \geq 2$  and  $1 \leq m < n$ . For any positive integer  $r$  dividing  $m$ , there are infinitely many integers  $\kappa$  and infinitely many integers  $\chi$  satisfying the following five conditions:*

- (i)  $\kappa$  satisfies (B3) – (B5) in Section 3.
- (ii)  $\kappa = 3^{2m-1} \kappa_*^r$  for some odd prime  $\kappa_*$  with  $\kappa_* \neq 3$ .
- (iii)  $\chi$  is an odd prime.
- (iv)  $(p, n, \kappa, \chi)$  satisfies (D1) – (D7) in Theorem 6.2.
- (v) let  $\mathcal{F}_{(\kappa, \chi)}^{(p, n, m, r)}$  be the generalized Fermat curve of signature  $(12n, 12n, 12n)$  defined by

$$(56) \quad \mathcal{F}_{(\kappa, \chi)}^{(p, n, m, r)} : 3^6 \kappa^6 x^{12n} - y^{12n} - p \chi^2 z^{12n} = 0.$$

Then  $\mathcal{F}_{(\kappa, \chi)}^{(p, n, m, r)}$  is a counterexample to the Hasse principle explained by the Brauer-Manin obstruction.

*Proof.* By Lemma 7.5, we see that for any positive integer  $r$  dividing  $m$ , there are infinitely many integers  $\kappa$  and infinitely many integers  $\chi$  satisfying (i), (ii), (iii) and (iv) in Corollary 7.6. For any couple  $(\kappa, \chi)$  satisfying (i), (ii), (iii) and (iv) in Corollary 7.6, applying Theorem 6.2 for the curve  $\mathcal{F}_{(\kappa, \chi)}^{(p, n, m, r)}$ , we deduce that  $\mathcal{F}_{(\kappa, \chi)}^{(p, n, m, r)}$  is a counterexample to the Hasse principle explained by the Brauer-Manin obstruction. Hence (v) in Corollary 7.6 holds, and thus our contention follows.  $\square$

## 8. THE DESCENDING CHAIN CONDITION ON SEQUENCES OF GENERALIZED FERMAT CURVES

In this section, we will study the descending chain condition on sequences of generalized Fermat curves. We will prove that there exist infinitely many sequences of generalized Fermat curves satisfying the descending chain condition in the sense of Definition 5.1. We begin by proving the main lemma in this section.

**Lemma 8.1.** *Let  $p$  be a prime such that  $p \equiv 1 \pmod{8}$  and  $p \equiv 2 \pmod{3}$ . Let  $n$  and  $m$  be positive integers such that  $2m < n$ . Then there exist an infinite set  $\mathbf{I}_{n, m}$  of integers and an infinite set  $\mathbf{J}_{n, m}$  of integers such that for each integer  $\kappa \in \mathbf{I}_{n, m}$  and each integer  $\chi \in \mathbf{J}_{n, m}$ ,  $\mathcal{F}_{(\kappa, \chi)}^{(m)}$  contains at least four rational points whereas  $\mathcal{F}_{(\kappa, \chi)}^{(n)}$  is a counterexample to the Hasse principle explained by the Brauer-Manin obstruction, where for each integer  $\kappa \in \mathbf{I}_{n, m}$  and each integer  $\chi \in \mathbf{J}_{n, m}$ ,  $\mathcal{F}_{(\kappa, \chi)}^{(m)}$  and  $\mathcal{F}_{(\kappa, \chi)}^{(n)}$  are the*

generalized Fermat curves of signatures  $(12m, 12m, 12m)$  and  $(12n, 12n, 12n)$ , respectively and defined by

$$(57) \quad \mathcal{F}_{(\kappa, \chi)}^{(m)} : 3^6 \kappa^6 x^{12m} - y^{12m} - p\chi^2 z^{12m} = 0$$

and

$$(58) \quad \mathcal{F}_{(\kappa, \chi)}^{(n)} : 3^6 \kappa^6 x^{12n} - y^{12n} - p\chi^2 z^{12n} = 0.$$

*Proof.* Let  $\mathbf{I}_{n,m}$  be the set of nonzero integers  $\kappa$  and  $\mathbf{J}_{n,m}$  be the set of integers  $\chi$  such that the following are true:

- (i)  $\kappa$  satisfies (B3) – (B5) in Section 3,
- (ii)  $\kappa = 3^{4m-1} \kappa_*^{2m}$  for some odd prime  $\kappa_*$  with  $\kappa_* \neq 3$ ,
- (iii)  $\chi$  is an odd prime, and
- (iv)  $(p, n, \kappa, \chi)$  satisfies (D1) – (D7) in Theorem 6.2.

Using Lemma 7.5 with  $(m, r)$  replaced by  $(2m, 2m)$ , we deduce that  $\mathbf{I}_{n,m}$  and  $\mathbf{J}_{n,m}$  are of infinite cardinality. Let  $\kappa$  be a nonzero integer in  $\mathbf{I}_{n,m}$ , and let  $\chi$  be an integer in  $\mathbf{J}_{n,m}$ . Let  $\mathcal{F}_{(\kappa, \chi)}^{(m)}$  and  $\mathcal{F}_{(\kappa, \chi)}^{(n)}$  be the generalized Fermat curves defined by (57) and (58), respectively. Since  $\kappa \in \mathbf{I}_{n,m}$ , there exists an odd prime  $\kappa_*$  such that  $\kappa_* \neq 3$  and  $\kappa = 3^{4m-1} \kappa_*^{2m}$ . The defining equation of  $\mathcal{F}_{(\kappa, \chi)}^{(m)}$  can be written in the form

$$\mathcal{F}_{(\kappa, \chi)}^{(m)} : (3^2 \kappa_* x)^{12m} - y^{12m} - p\chi^2 z^{12m} = 0.$$

Hence we see that the points  $(x, y, z) = \left( \pm \frac{1}{3^2 \kappa_*}, \pm 1, 0 \right)$  belong to  $\mathcal{F}_{(\kappa, \chi)}^{(m)}(\mathbb{Q})$ , and thus  $\mathcal{F}_{(\kappa, \chi)}^{(m)}$  has at least four  $\mathbb{Q}$ -rational points.

Since  $\kappa \in \mathbf{I}_{n,m}$  and  $\chi \in \mathbf{J}_{n,m}$ , we know that  $\kappa$  satisfies (B3) – (B5) in Section 3 and the quadruple  $(p, n, \kappa, \chi)$  satisfies (D1) – (D7) in Theorem 6.2. By Theorem 6.2, we deduce that  $\mathcal{F}_{(\kappa, \chi)}^{(n)}$  is a counterexample to the Hasse principle explained by the Brauer-Manin obstruction. Thus our contention follows.  $\square$

**Remark 8.2.** Let  $(p, n, \kappa, \chi)$  be the quadruple satisfying the conditions in Theorem 6.2, and assume further that  $n \geq 3$ . Let  $\mathcal{F}$  be the generalized Fermat curve defined as in Theorem 6.2. By Lemma 8.1 and using the same arguments as in Remark 5.4, we deduce that the signature  $(12n, 12n, 12n)$  of  $\mathcal{F}$  is *optimal* in the sense that in Theorem 6.2, one can not replace  $n$  by a positive divisor  $m$  of  $n$  with  $m \neq n$ .

We now prove the main result in this section, which says that there are infinitely many sequences of generalized Fermat curves that satisfy the DCC of arbitrary length.

**Corollary 8.3.** *Let  $h$  be a positive integer. Then there exist infinitely many sequences of generalized Fermat curves that satisfy the DCC of length  $h$  in the sense of Definition 5.1.*

*Proof.* Let  $p$  be a prime such that  $p \equiv 1 \pmod{8}$  and  $p \equiv 2 \pmod{3}$ . Let  $n_0$  and  $n_1$  be integers such that  $n_0 \geq 3$  and  $n_1 \geq 1$ . Set

$$\begin{aligned} n &:= n_0^h n_1, \\ m &:= n_0^{h-1} n_1. \end{aligned}$$

Since  $n_0 \geq 3$ , we see that

$$2m = 2n_0^{h-1} n_1 < n_0 n_0^{h-1} n_1 = n.$$

Applying Lemma 8.1 for the triple  $(p, n, m)$ , we deduce that there exist an infinite set  $\mathbf{I}_{n,m}$  of integers and an infinite set  $\mathbf{J}_{n,m}$  of integers such that for each integer  $\kappa \in \mathbf{I}_{n,m}$  and each integer  $\chi \in \mathbf{J}_{n,m}$ ,  $\mathcal{F}_{(\kappa, \chi)}^{(\kappa, \chi)}$  contains at least four rational points whereas  $\mathcal{F}_h^{(\kappa, \chi)}$  is a counterexample to the Hasse principle

explained by the Brauer-Manin obstruction, where for each integer  $\kappa \in \mathbf{I}_{n,m}$  and each integer  $\chi \in \mathbf{J}_{n,m}$ ,  $\mathcal{F}_{h-1}^{(\kappa,\chi)}$  and  $\mathcal{F}_h^{(\kappa,\chi)}$  are the generalized Fermat curves defined by

$$\mathcal{F}_{h-1}^{(\kappa,\chi)} : 3^6 \kappa^6 x^{12n_0^{h-1}n_1} - y^{12n_0^{h-1}n_1} - p\chi^2 z^{12n_0^{h-1}n_1} = 0$$

and

$$\mathcal{F}_h^{(\kappa,\chi)} : 3^6 \kappa^6 x^{12n_0^h n_1} - y^{12n_0^h n_1} - p\chi^2 z^{12n_0^h n_1} = 0,$$

respectively.

Take any nonzero integer  $\kappa \in \mathbf{I}_{n,m}$ , and let  $\chi$  be any nonzero integer in  $\mathbf{J}_{n,m}$ . For each integer  $i \geq 1$ , let  $\mathcal{F}_i^{(\kappa,\chi)}$  be the generalized Fermat curve defined by

$$\mathcal{F}_i^{(\kappa,\chi)} : 3^6 \kappa^6 x^{12n_0^i n_1} - y^{12n_0^i n_1} - p\chi^2 z^{12n_0^i n_1} = 0,$$

and for each integer  $i \geq 1$ , let  $\psi_i^{(\kappa,\chi)} : \mathcal{F}_{i+1}^{(\kappa,\chi)} \rightarrow \mathcal{F}_i^{(\kappa,\chi)}$  be the  $\mathbb{Q}$ -morphism of curves defined by

$$\begin{aligned} \psi_i^{(\kappa,\chi)} : \mathcal{F}_{i+1}^{(\kappa,\chi)} &\rightarrow \mathcal{F}_i^{(\kappa,\chi)} \\ (x, y, z) &\mapsto (x^{n_0}, y^{n_0}, z^{n_0}). \end{aligned}$$

We contend that the sequence  $(\mathcal{F}_i^{(\kappa,\chi)}, \psi_i^{(\kappa,\chi)})_{i \geq 1}$  satisfies the DCC of length  $h$  in the sense of Definition

5.1. Indeed, since  $\kappa \in \mathbf{I}_{n,m}$  and  $\chi \in \mathbf{J}_{n,m}$ , we know that  $\mathcal{F}_{h-1}^{(\kappa,\chi)}$  contains at least four rational points whereas  $\mathcal{F}_h^{(\kappa,\chi)}$  is a counterexample to the Hasse principle explained by the Brauer-Manin obstruction. Thus (DCC2) in Definition 5.1 holds.

Let  $(x_0, y_0, z_0)$  be any rational point in  $\mathcal{F}_{h-1}^{(\kappa,\chi)}(\mathbb{Q})$ . We see that for each integer  $1 \leq i \leq h-2$ , the point  $(x, y, z) = (x_0^{n_0^{h-1-i}}, y_0^{n_0^{h-1-i}}, z_0^{n_0^{h-1-i}})$  belongs to  $\mathcal{F}_i^{(\kappa,\chi)}(\mathbb{Q})$ . Hence (DCC1) in Definition 5.1 holds. For each integer  $i \geq 1$ , let  $g_i^{(\kappa,\chi)}$  denote the genus of the curve  $\mathcal{F}_i^{(\kappa,\chi)}$ . We see that

$$g_i^{(\kappa,\chi)} = (12n_0^i n_1 - 1)(6n_0^i n_1 - 1)$$

for each  $i \geq 1$ . Hence it follows that  $g_i^{(\kappa,\chi)} < g_j^{(\kappa,\chi)}$  for any positive integers  $i, j$  with  $1 \leq i < j$ , and thus (DCC3) holds. Therefore  $(\mathcal{F}_i^{(\kappa,\chi)}, \psi_i^{(\kappa,\chi)})_{i \geq 1}$  satisfies the DCC of length  $h$  in the sense of Definition 5.1. Since  $\mathbf{I}_{n,m}$  and  $\mathbf{J}_{n,m}$  are of infinite cardinality, our contention follows.  $\square$

**Remark 8.4.** Note that there exist infinitely many sequences of generalized Fermat curves that do not satisfy the DCC of any length. Indeed, take any triple  $(A, B, C)$  of nonzero integers such that  $A + B + C = 0$ . Let  $n$  be an integer such that  $n \geq 2$ . For each integer  $i \geq 1$ , let  $\mathcal{F}_i$  be the generalized Fermat curve defined by

$$\mathcal{F}_i : Ax^{n^i} + By^{n^i} + Cz^{n^i} = 0,$$

and for each integer  $i \geq 1$ , let  $\psi_i : \mathcal{F}_{i+1} \rightarrow \mathcal{F}_i$  be the morphism of curves defined by

$$\begin{aligned} \psi_i : \mathcal{F}_{i+1} &\rightarrow \mathcal{F}_i \\ (x, y, z) &\mapsto (x^n, y^n, z^n). \end{aligned}$$

Since  $A + B + C = 0$ , we deduce that for each  $i \geq 1$ , the curve  $\mathcal{F}_i$  contains the rational point  $(x, y, z) = (1, 1, 1)$ , and hence  $\mathcal{F}_i(\mathbb{Q}) \neq \emptyset$  for each integer  $i \geq 1$ . Thus the sequence  $(\mathcal{F}_i, \psi_i)_{i \geq 1}$  does not satisfy the DCC.

## 9. EPILOGUE

In Sections 4 and 6, for each positive integer  $n \geq 2$ , we have constructed certain families of generalized Mordell curves of degree  $12n$  and certain families of generalized Fermat curves of signature  $(12n, 12n, 12n)$  arising from rational points of the subset of  $\mathcal{X}_p(\mathbb{Q})$  defined by (14) in Section 3 that are counterexamples to the Hasse principle explained by the Brauer-Manin obstruction. Because of condition (B3) in Section 3, it is impossible to construct generalized Mordell curves of degree 12 and certain families of generalized Fermat curves of signature  $(12, 12, 12)$  that are counterexamples to the Hasse principle; in other words, we rule out the case  $n = 1$  in Theorems 4.2 and 6.2. In this section, we will introduce another subset of the set of rational points on  $\mathcal{X}_p$ , which allows us to include the case  $n = 1$  in Theorems 4.2 and 6.2. Using this subset of the set of rational points on  $\mathcal{X}_p$  and assuming Schinzel's Hypothesis H, we will prove that for each prime  $p$  such that  $p \equiv 1 \pmod{8}$  and  $p \equiv 2 \pmod{3}$  and each integer  $n \geq 1$ , there should be infinitely many septuples  $(A, B, C, D, E, F, G)$  of integers that satisfy Hypothesis FM with respect to the couple  $(p, n)$  in the sense of Definition 1.1. Using these septuples and repeating the same arguments as in Sections 4 and 6, one can show that for each  $n \geq 1$ , there should exist families of generalized Mordell curves of degree  $12n$  and families of generalized Fermat curves of signature  $(12n, 12n, 12n)$  that are counterexamples to the Hasse principle explained by the Brauer-Manin obstruction.

In this section, we restrict ourselves to describing a new subset of  $\mathcal{X}_p(\mathbb{Q})$  for each prime  $p$  that allows us to produce new families of generalized Mordell curves and new families of generalized Fermat curves that are counterexamples to the Hasse principle, but not proceeding to describe these families of curves. The interested reader can use similar arguments as in Sections 4 and 6 to construct new families of generalized Mordell curves and new families of generalized Fermat curves arising from new rational points in  $\mathcal{X}_p(\mathbb{Q})$  for each prime  $p$  that are counterexamples to the Hasse principle explained by the Brauer-Manin obstruction. We begin by introducing a new subset of  $\mathcal{X}_p(\mathbb{Q})$  for each prime  $p$  such that  $p \equiv 1 \pmod{8}$  and  $p \equiv 2 \pmod{3}$ .

Let  $p$  be an odd prime such that  $p \neq 3$ . Let  $\lambda$  and  $\gamma$  be nonzero *odd integers* such that

$$\gcd(\lambda, 3\gamma) = \gcd(p, 3\gamma) = \gcd(p, \lambda) = 1.$$

Since  $\gcd(p\lambda^2, 9\gamma^2) = 1$ , there exist nonzero integers  $\epsilon_0$  and  $\delta_0$  such that

$$p\lambda^2\epsilon_0 + 9\gamma^2\delta_0 = 1.$$

For integers  $\mu, t_0, F_0 \in \mathbb{Z}$ , we define

$$(59) \quad \begin{cases} A &:= \frac{p\lambda^2 - 9\gamma^2}{2} \\ B &:= 2pF_0^2(\delta_0 - \epsilon_0 - \mu(p\lambda^2 + 9\gamma^2)) + (p\lambda^2 + 9\gamma^2)t_0F_0 \\ C &:= 2pF_0^2(\delta_0 + \epsilon_0 - \mu(p\lambda^2 - 9\gamma^2)) + (p\lambda^2 - 9\gamma^2)t_0F_0 \\ D &= \frac{p\lambda^2 + 9\gamma^2}{2} \\ E &:= F_0(2pF_0(\epsilon_0 + 9\mu\gamma^2) - 9\gamma^2t_0)(2F_0(\delta_0 - p\mu\lambda^2) + \lambda^2t_0) \\ F &:= 2F_0 \\ G &= 3\lambda\gamma. \end{cases}$$

Note that  $B$  and  $C$  can be written in the following form

$$(60) \quad \begin{cases} B &:= 2pF_0^2(\delta_0 - \epsilon_0 - 2\mu D) + 2Dt_0F_0 \\ C &:= 2pF_0^2(\delta_0 + \epsilon_0 - 2\mu A) + 2At_0F_0. \end{cases}$$

It is not difficult to verify that the point  $\mathcal{P} := (a : b : c : d : e : f : g) = (A : B : C : D : E : F : G)$  belongs to  $\mathcal{X}_p(\mathbb{Q})$ ; hence, the septuple  $(A, B, C, D, E, F, G)$  satisfies (A1) in Definition 1.1. We see that (59) defines the parametrization of a subset of  $\mathcal{X}_p(\mathbb{Q})$  by parameters  $\lambda, \gamma, \mu, t_0$  and  $F_0$ . Using this parametrization, we will show that there are infinitely many septuples  $(A, B, C, D, E, F, G)$  satisfying Hypothesis FM with respect to the couples  $(p, n)$ , where  $n$  is a sufficiently large integer. The following lemma is the main result in this section.

**Lemma 9.1.** *Let  $p$  be a prime such that  $p \equiv 1 \pmod{8}$  and  $p \equiv 2 \pmod{3}$ . Then there exist infinitely many septuples  $(A, B, C, D, E, F, G) \in \mathbb{Z}^7$  such that they satisfy (59) and (A1), (A3), (A4), (A5), (A7) in Definition 1.1, and such that for any integer  $n \geq 1$ , they satisfy (A6) in Definition 1.1 with respect to the couple  $(p, n)$ .*

*Proof.* Let  $\lambda$  and  $\gamma$  be odd integers such that

$$(61) \quad \gcd(\lambda, 3\gamma) = \gcd(p, 3\gamma) = \gcd(p, \lambda) = 1.$$

Since  $\gcd(p\lambda^2, 9\gamma^2) = 1$ , there exist non-zero integers  $\epsilon^*$  and  $\delta^*$  such that

$$p\lambda^2\epsilon^* + 9\gamma^2\delta^* = 1.$$

We see that  $\epsilon_0 = \epsilon^* + 9\gamma^2s^*$  and  $\delta_0 = \delta^* - p\lambda^2s^*$  satisfy the following equation

$$(62) \quad p\lambda^2\epsilon_0 + 9\gamma^2\delta_0 = 1,$$

where  $s^*$  is an arbitrary integer. For our purpose, we choose  $s^*$  such that  $\delta^* + s^* \equiv 2 \pmod{3}$ . Since  $\lambda \not\equiv 0 \pmod{3}$  and  $p \equiv 2 \pmod{3}$ , we deduce that

$$(63) \quad \delta_0 = \delta^* - p\lambda^2s^* \equiv \delta^* - 2s^* \equiv \delta^* + s^* \equiv 2 \pmod{3}.$$

Let  $(A, B, C, D, E, F, G)$  be the septuple of integers defined by (59), where  $\mu, t_0$  and  $F_0$  will be determined later. It is not difficult to prove that  $(A, B, C, D, E, F, G)$  belongs to  $X_p(\mathbb{Q})$ , where  $X_p$  is the threefold defined by (2), and hence it satisfies (A1) in Definition 1.1. By (59) and (60), we see that

$$\begin{aligned} AC - BD &= A(2pF_0^2(\delta_0 + \epsilon_0 - 2\mu A) + 2At_0F_0) - D(2pF_0^2(\delta_0 - \epsilon_0 - 2\mu D) + 2Dt_0F_0) \\ &= 4pF_0^2(D^2 - A^2)\mu + 2pF_0^2(A(\delta_0 + \epsilon_0) - D(\delta_0 - \epsilon_0)) + 2t_0F_0(A^2 - D^2) \\ &= 4p^2F_0^2G^2\mu + 2pF_0^2(\epsilon_0(A + D) + \delta_0(A - D)) - 2pt_0F_0G^2 \quad (\text{since } A^2 - D^2 + pG^2 = 0) \\ &= 2pF_0(2pF_0G^2\mu + F_0(\epsilon_0(A + D) + \delta_0(A - D)) - t_0G^2) \\ (64) \quad &= 2pF_0Q^*. \end{aligned}$$

Here,

$$Q^* = 2pF_0G^2\mu + F_0(\epsilon_0(A + D) + \delta_0(A - D)) - t_0G^2.$$

By (59), we see that

$$\begin{aligned} A + D &= p\lambda^2, \\ A - D &= -9\gamma^2. \end{aligned}$$

By the above identities, (62), and since  $G = 3\lambda\gamma$ , we deduce that

$$\begin{aligned} Q^* &= 2pF_0G^2\mu + F_0(p\lambda^2\epsilon_0 - 9\gamma^2\delta_0) - t_0G^2 \\ &= 2pF_0G^2\mu + F_0(2p\lambda^2\epsilon_0 - 1) - t_0G^2 \\ (65) \quad &= (18p\lambda^2\gamma^2F_0)\mu + F_0(2p\lambda^2\epsilon_0 - 1) - 9\lambda^2\gamma^2t_0. \end{aligned}$$

★ *Step 1. Choosing  $t_0$ .*

We define

$$(66) \quad t_0 := -3\lambda\gamma F_0 t_1,$$

where  $t_1$  is an integer which will be chosen below in this step, and  $F_0$  will be chosen in *Step 2*. By (65), one can write  $Q^*$  in the form

$$(67) \quad Q^* = F_0((18p\lambda^2\gamma^2)\mu + 2p\lambda^2\epsilon_0 - 1 + 27\lambda^3\gamma^3t_1) = F_0(P_1^*\mu + R_1^*),$$

where

$$(68) \quad \begin{cases} P_1^* := 18p\lambda^2\gamma^2, \\ R_1^* := 2p\lambda^2\epsilon_0 - 1 + 27\lambda^3\gamma^3t_1. \end{cases}$$



Since  $\gcd(27\lambda^3\gamma^3, p) = 1$ , there exist non-zero integers  $t_2$  and  $t_3$  such that

$$(69) \quad 27\lambda^3\gamma^3 t_2 - pt_3 = 1.$$

Take any non-zero integer  $\pi$  such that  $\pi$  is a *quadratic residue* in  $\mathbb{F}_p^\times$ , and let  $t_5$  be any non-zero integer such that

$$(70) \quad \begin{cases} t_5 \equiv \frac{\pi - 2\lambda^2\epsilon_0 - t_3}{27\lambda^3\gamma^3} \pmod{p} \\ t_5 \equiv 1 - t_3 \pmod{2}. \end{cases}$$

Note that there are infinitely many such integers  $\pi$  and  $t_5$ . Define

$$(71) \quad t_1 := t_2 + pt_5,$$

and

$$(72) \quad t_4 := t_3 + 27\lambda^3\gamma^3 t_5.$$

By (69), (71) and (72), we see that

$$(73) \quad 27\lambda^3\gamma^3 t_1 - pt_4 = 1.$$

In summary, by (66) and (71),  $t_0$  is of the form

$$(74) \quad t_0 = -3\lambda\gamma F_0(t_2 + pt_5),$$

where  $t_2$  is an integer satisfying (69) and  $t_5$  is any non-zero integer satisfying (70).

★ *Step 2. Choosing  $F_0$ .*

Define

$$(75) \quad u := \begin{cases} 1 & \text{if } \lambda\gamma \text{ is a quadratic residue modulo } p, \\ 0 & \text{if } \lambda\gamma \text{ is a quadratic non-residue modulo } p. \end{cases}$$

We take  $F_0$  to be any non-zero integer such that the following are true:

(F1)  $F_0 = 3^u F_1$ , where  $F_1$  is an integer such that  $\gcd(F_1, 3) = \gcd(F_1, p) = 1$ .

(F2)  $p$  is a square in  $\mathbb{Q}_l^\times$  for each odd prime  $l$  dividing  $F_1$ .

★ *Step 3. Defining  $H$ .*

We prove that  $\frac{3\lambda\gamma}{F_0}$  is a quadratic residue in  $\mathbb{F}_p^\times$ . Assume first that  $\lambda\gamma$  is a quadratic residue in  $\mathbb{F}_p^\times$ . By (75) in *Step 2*, we know that  $u = 1$ . By (F1) in *Step 2*, we see that

$$\frac{3\lambda\gamma}{F_0} = \frac{3\lambda\gamma}{3^u F_1} = \frac{\lambda\gamma}{F_1}.$$

Hence, in order to prove that  $\frac{3\lambda\gamma}{F_0}$  is a quadratic residue in  $\mathbb{F}_p^\times$ , it suffices to prove that  $F_1$  is a square in  $\mathbb{F}_p^\times$ . Write  $F_1$  in the form

$$F_1 = 2^{v_2(F_1)} \prod_{l|F_1} l^{v_l(F_1)},$$

where the product is taken over all odd prime  $l$  dividing  $F_1$ . Since  $p \equiv 1 \pmod{8}$ , we know that 2 is a quadratic residue in  $\mathbb{F}_p^\times$ . Hence it follows from (F2) in *Step 2* and the quadratic reciprocity law that

$$\begin{aligned} \left(\frac{F_1}{p}\right) &= \left(\frac{2^{v_2(F_1)} \prod_{l|F_1} l^{v_l(F_1)}}{p}\right) \\ &= \left(\frac{2^{v_2(F_1)}}{p}\right) \prod_{l|F_1} \left(\frac{l^{v_l(F_1)}}{p}\right) \\ &= \left(\frac{2}{p}\right)^{v_2(F_1)} \prod_{l|F_1} \left(\frac{p}{l}\right)^{v_l(F_1)} \\ &= 1. \end{aligned}$$

Thus  $F_1$  is a quadratic residue in  $\mathbb{F}_p^\times$ , and hence  $\frac{3\lambda\gamma}{F_0}$  is a quadratic residue in  $\mathbb{F}_p^\times$ .

Assume now that  $\lambda\gamma$  is a quadratic non-residue in  $\mathbb{F}_p^\times$ . By (75) in *Step 2*, we know that  $u = 0$ . Hence  $3^u = 1$ , and hence  $F_0 = 3^u F_1 = F_1$ . As was shown above,  $F_1$  is a square in  $\mathbb{F}_p^\times$ , and thus  $F_0$  is a square in  $\mathbb{F}_p^\times$ . Since  $p \equiv 2 \pmod{3}$ , we deduce that  $p$  is a quadratic non-residue in  $\mathbb{F}_3^\times$ . By the quadratic reciprocity law, we deduce that  $3$  is a quadratic non-residue in  $\mathbb{F}_p^\times$ . Thus  $3\lambda\gamma$  is a square in  $\mathbb{F}_p^\times$ , and therefore it follows that  $\frac{3\lambda\gamma}{F_0}$  is a quadratic residue in  $\mathbb{F}_p^\times$ .

Therefore, in any event,  $\frac{3\lambda\gamma}{F_0}$  is a square in  $\mathbb{F}_p^\times$ . We now define  $H$  to be any non-zero integer such that

$$(76) \quad H \equiv \left( \frac{3\lambda\gamma}{F_0} \right)^{1/2} \pmod{p}.$$

★ *Step 4. Defining  $\mu$ .*

By (68) and (73),  $R_1^*$  can be written in the form

$$R_1^* = 2p\lambda^2\epsilon_0 - 1 + 27\lambda^3\gamma^3t_1 = 2p\lambda^2\epsilon_0 + pt_4 = pR_2^*,$$

where

$$(77) \quad R_2^* := 2\lambda^2\epsilon_0 + t_4.$$

By (67) and (68), we can write  $Q^*$  in the form

$$(78) \quad Q^* = F_0(P_1^*\mu + R_1^*) = pF_0(P_2^*\mu + R_2^*) = pF_0Q_1^*,$$

where

$$(79) \quad Q_1^* = P_2^*\mu + R_2^*$$

and

$$(80) \quad P_2^* = 18\lambda^2\gamma^2.$$

We contend that  $\gcd(3pP_2^*, R_2^*) = 1$ . Since  $\lambda$  and  $\gamma$  is odd, it follows from (70), (72) and (77) that

$$(81) \quad R_2^* \equiv t_4 \equiv t_3 + 27\lambda^3\gamma^3t_5 \equiv t_3 + t_5 \equiv 1 \pmod{2}.$$

Since  $\gcd(p, \lambda) = 1$ , it follows from (73) and (77) that

$$(82) \quad R_2^* \equiv t_4 \equiv -\frac{1}{p} \not\equiv 0 \pmod{l}$$

for each odd prime  $l$  dividing  $\lambda$ , and hence  $\gcd(R_2^*, \lambda) = 1$ . Since  $\gcd(p, 3\gamma) = 1$ , it follows from (62), (73) and (77) that

$$(83) \quad R_2^* = 2\lambda^2\epsilon_0 + t_4 \equiv \frac{2}{p} + t_4 \equiv \frac{2}{p} - \frac{1}{p} \equiv \frac{1}{p} \not\equiv 0 \pmod{l}$$

for each odd prime  $l$  dividing  $3\gamma$ , and hence  $\gcd(R_2^*, 3\gamma) = 1$ . By (70), (72) and (77), we see that

$$(84) \quad R_2^* = 2\lambda^2\epsilon_0 + t_4 = 2\lambda^2\epsilon_0 + t_3 + 27\lambda^3\gamma^3t_5 \equiv \pi \not\equiv 0 \pmod{p},$$

and hence  $\gcd(R_2^*, p) = 1$ . Since  $P_2^* = 18\lambda^2\gamma^2$ , it follows from (81), (82), (83) and (84) that

$$\gcd(3pP_2^*, R_2^*) = 1.$$

We now define  $\mu$ . Since  $\gcd(3pP_2^*, R_2^*) = 1$ , it follows from the Dirichlet's theorem on arithmetic progressions that there are infinitely many integers  $\mu_1$  such that  $3pP_2^*\mu_1 + R_2^*$  is an odd prime. Take such an integer  $\mu_1$ , and define

$$(85) \quad \mu = 3p\mu_1.$$

By (79), the choice of  $\mu_1$  and the definition of  $\mu$ , we see that  $Q_1^*$  is an odd prime.

★ *Step 5. Verifying (A3).*

By (59) and (61), we see that  $\gcd(A, D, G) = 1$  and  $G \not\equiv 0 \pmod{p}$ . Hence, it remains to verify that  $E \not\equiv 0 \pmod{p}$ . We see that

$$\begin{aligned}
 E &= F_0(2pF_0(\epsilon_0 + 9\mu\gamma^2) - 9\gamma^2t_0)(2F_0(\delta_0 - p\mu\lambda^2) + \lambda^2t_0) \quad (\text{by (59)}) \\
 &\equiv -9\gamma^2F_0t_0(\lambda^2t_0 + 2\delta_0F_0) \\
 &\equiv 27\lambda\gamma^3F_0^2t_2(-3\lambda^3\gamma F_0t_2 + 2\delta_0F_0) \quad (\text{by (74)}) \\
 &\equiv -27\lambda\gamma^3F_0^3t_2\left(3\lambda^3\gamma t_2 - \frac{2}{9\gamma^2}\right) \quad (\text{by (62)}) \\
 &\equiv -\frac{F_0^3}{\lambda^2}\left(\frac{1}{9\gamma^2} - \frac{2}{9\gamma^2}\right) \quad (\text{by (69)}) \\
 &\equiv \frac{F_0^3}{9\lambda^2\gamma^2} \not\equiv 0 \pmod{p}.
 \end{aligned} \tag{86}$$

Hence (A3) holds.

★ *Step 6. Verifying (A4).*

Let  $l$  be any odd prime such that  $\gcd(l, 3) = \gcd(l, p) = 1$  and  $l$  divides  $AC - BD$ . We will prove that  $p$  is a square in  $\mathbb{Q}_l^\times$ . Indeed, by (64) and (78), we can write  $AC - BD$  in the form

$$AC - BD = 2pF_0Q^* = 2p^2F_0^2Q_1^*, \tag{87}$$

where  $Q_1^*$  is given by (79). Recall that by the choice of  $\mu$  in *Step 4*,  $Q_1^*$  is an odd prime. If  $l$  divides  $F_0$ , then it follows from (F1) in *Step 2* that  $l$  divides  $F_1$ . Hence it follows from (F2) in *Step 2* that  $p$  is a square in  $\mathbb{Q}_l^\times$ . If  $\gcd(l, F_0) = 1$ , we see that since  $Q_1^*$  is an odd prime,  $l$  divides  $AC - BD$  and  $\gcd(l, 2pF_0) = 1$ , it follows from (87) that  $l = Q_1^*$ . Hence it suffices to show that  $p$  is a square in  $\mathbb{Q}_{Q_1^*}^\times$ , where  $\mathbb{Q}_{Q_1^*}$  denotes the  $Q_1^*$ -adic field.

By (79), (84) and (85), we see that

$$Q_1^* = P_2^*\mu + R_2^* = 3pP_2^*\mu_1 + R_2^* \equiv R_2^* \equiv \pi \pmod{p}.$$

By the choice of  $\pi$  in *Step 1*, we know that  $\pi$  is a quadratic residue in  $\mathbb{F}_p^\times$ . Hence it follows from the last congruence that  $\left(\frac{Q_1^*}{p}\right) = 1$ , where  $\left(\frac{\cdot}{\cdot}\right)$  denotes the Jacobi symbol. By the quadratic reciprocity law, we see that

$$\left(\frac{p}{Q_1^*}\right) = \left(\frac{Q_1^*}{p}\right) = 1,$$

and thus  $p$  is a square in  $\mathbb{Q}_{Q_1^*}^\times$ . Hence (A4) holds.

★ *Step 7. Verifying (A5).*

Since  $p \equiv 2 \pmod{3}$ ,  $p$  is a quadratic non-residue in  $\mathbb{F}_3^\times$ . By the quadratic reciprocity law, we deduce that 3 is a quadratic non-residue in  $\mathbb{F}_p^\times$ , and hence  $-3$  is not a square in  $\mathbb{F}_p^\times$ . Thus the group of all cube roots of unity in  $\mathbb{F}_p^\times$  is trivial. We will prove that  $H$  satisfies (A5), where  $H$  is defined in *Step 3*. Note that since the group of all cube roots of unity in  $\mathbb{F}_p^\times$  is trivial, the second condition in (A5) is tantamount to saying that  $A + BH^4$  is a quadratic non-residue in  $\mathbb{F}_p^\times$ .

By (59), (76) and (86), we see that

$$\begin{aligned}
 G - EH^6 &\equiv 3\lambda\gamma - \left(\frac{F_0^3}{9\lambda^2\gamma^2}\right)\left(\frac{27\lambda^3\gamma^3}{F_0^3}\right) \\
 &\equiv 3\lambda\gamma - 3\lambda\gamma \equiv 0 \pmod{p}.
 \end{aligned}$$

We see that

$$\begin{aligned}
A + BH^4 &\equiv -\frac{9\gamma^2}{2} + 9\gamma^2 t_0 F_0 \left( \frac{9\lambda^2 \gamma^2}{F_0^2} \right) \quad (\text{by (59) and (76)}) \\
&\equiv -\frac{9\gamma^2}{2} + 9\gamma^2 (-3\lambda\gamma F_0(t_2 + pt_5)) F_0 \left( \frac{9\lambda^2 \gamma^2}{F_0^2} \right) \quad (\text{by (74)}) \\
&\equiv -\frac{9\gamma^2}{2} - 27\lambda\gamma^3 F_0^2 t_2 \left( \frac{9\lambda^2 \gamma^2}{F_0^2} \right) \\
&\equiv -\frac{9\gamma^2}{2} - (27\lambda^3 \gamma^3 t_2) 9\gamma^2 \\
&\equiv -\frac{9\gamma^2}{2} - 9\gamma^2 \quad (\text{by (69)}) \\
&\equiv 3 \left( \frac{-1}{2} \right) (3\gamma)^2 \pmod{p}.
\end{aligned}$$

Since  $-1$  and  $2$  are quadratic residues in  $\mathbb{F}_p^\times$  and  $3$  is a quadratic non-residue in  $\mathbb{F}_p^\times$ , we deduce that  $3 \left( \frac{-1}{2} \right) (3\gamma)^2$  is a quadratic non-residue in  $\mathbb{F}_p^\times$ . Hence  $A + BH^4$  is a quadratic non-residue in  $\mathbb{F}_p^\times$ , and thus (A5) holds.

★ *Step 8. Verifying (A6).*

Since  $\lambda \not\equiv 0 \pmod{3}$  and  $p \equiv 2 \pmod{3}$ , it follows from (62) that

$$(88) \quad \epsilon_0 \equiv \frac{1}{p\lambda^2} \equiv \frac{1}{2} \equiv 2 \pmod{3}.$$

By (59) and (74), we see that

$$\begin{aligned}
E &= F_0(2pF_0(\epsilon_0 + 9\mu\gamma^2) - 9\gamma^2 t_0)(2F_0(\delta_0 - p\mu\lambda^2) + \lambda^2 t_0) \\
&= F_0(2pF_0(\epsilon_0 + 9\mu\gamma^2) - 9\gamma^2(-3\lambda\gamma F_0(t_2 + pt_5)))(2F_0(\delta_0 - p\mu\lambda^2) + \lambda^2(-3\lambda\gamma F_0(t_2 + pt_5))) \quad (\text{by (74)}) \\
&= F_0^3(2p(\epsilon_0 + 9\mu\gamma^2) + 27\lambda\gamma^3(t_2 + pt_5))(2(\delta_0 - p\mu\lambda^2) - 3\lambda^3\gamma(t_2 + pt_5)).
\end{aligned}$$

Hence we deduce that

$$(89) \quad v_3(E) = v_3(F_0^3) + v_3(2p(\epsilon_0 + 9\mu\gamma^2) + 27\lambda\gamma^3(t_2 + pt_5)) + v_3(2(\delta_0 - p\mu\lambda^2) - 3\lambda^3\gamma(t_2 + pt_5)).$$

By (F1) in *Step 2*, we see that

$$(90) \quad v_3(F_0^3) = 3v_3(F_0) = 3v_3(3^u F_1) = 3v_3(3^u) + 3v_3(F_1) = 3u.$$

By (88) and since  $p \equiv 2 \pmod{3}$ , we see that

$$2p(\epsilon_0 + 9\mu\gamma^2) + 27\lambda\gamma^3(t_2 + pt_5) \equiv 2p\epsilon_0 \equiv 8 \equiv 2 \pmod{3},$$

and hence

$$(91) \quad v_3(2p(\epsilon_0 + 9\mu\gamma^2) + 27\lambda\gamma^3(t_2 + pt_5)) = 0.$$

By (85), we see that

$$\mu = 3p\mu_1 \equiv 0 \pmod{3},$$

and hence it follows from (63) that

$$2(\delta_0 - p\mu\lambda^2) - 3\lambda^3\gamma(t_2 + pt_5) \equiv 2\delta_0 \equiv 4 \equiv 1 \pmod{3}.$$

Thus we deduce that

$$(92) \quad v_3(2(\delta_0 - p\mu\lambda^2) - 3\lambda^3\gamma(t_2 + pt_5)) = 0.$$

Hence it follows from (89), (90), (91) and (92) that

$$v_3(E) = 3u,$$

and thus we deduce from (59), (61) and (75) that

$$v_3(E) - v_3(G) = 3u - v_3(3\lambda\gamma) = 3u - 1 \leq 3 - 1 = 2 < 3n$$

for any integer  $n \geq 1$ . Therefore (A6) holds.

★ *Step 9. Verifying (A7).*

By (74), we know that

$$t_0 = -3\lambda\gamma F_0(t_2 + pt_5) \equiv 0 \pmod{3}.$$

Since  $p \equiv 2 \pmod{3}$ ,  $\lambda \not\equiv 0 \pmod{3}$  and  $\mu = 3p\mu_1 \equiv 0 \pmod{3}$ , it follows from (59), (61), (63) and (88) that

$$\begin{aligned} A + B &\equiv \frac{p\lambda^2}{2} + 2pF_0^2(\delta_0 - \epsilon_0) \\ &\equiv 1 + 4F_0^2(2 - 2) \equiv 1 \not\equiv 0 \pmod{3}. \end{aligned}$$

By (59), we know that

$$G = 3\lambda\gamma \equiv 0 \pmod{3}.$$

Hence (A7) holds.

Therefore, by what we have shown above, our contention follows.  $\square$

**Remark 9.2.** Lemma 9.1 shows that for a prime  $p$  with  $p \equiv 1 \pmod{8}$  and  $p \equiv 2 \pmod{3}$  and an integer  $n \geq 1$ , there are infinitely many septuples  $(A, B, C, D, E, F, G)$  defined by (59) that satisfy (A1), (A3), (A4), (A5), (A6) and (A7) with respect to the couple  $(p, n)$ . It is not difficult to choose  $n$  sufficiently large so that the septuples  $(A, B, C, D, E, F, G)$  in Lemma 9.1 satisfy Hypothesis FM with respect to the couple  $(p, n)$ . Such septuples produce infinitely many generalized Mordell curves of degree  $12n$  that have no  $\mathbb{Q}$ -rational points. More precisely, we prove the following.

**Corollary 9.3.** *Let  $p$  be a prime such that  $p \equiv 1 \pmod{8}$  and  $p \equiv 2 \pmod{3}$ . There exists an infinite set  $\mathfrak{C}_p \subseteq \mathbb{Z}^7$  consisting of the septuples  $(A, B, C, D, E, F, G) \in \mathbb{Z}^7$  defined by (59) that satisfy (A1), (A3), (A4), (A5), (A7) in Definition 1.1. Furthermore, for each septuple  $\mathcal{T} := (A, B, C, D, E, F, G) \in \mathfrak{C}_p$ , there exists a positive real number  $n_{E,G} \geq 1$  such that for any integer  $n > n_{E,G}$ , the septuple  $\mathcal{T}$  satisfies Hypothesis FM with respect to  $(p, n)$  in the sense of Definition 1.1, and the smooth projective model  $\mathcal{C}_{n,\mathcal{T}}$  of the affine curve defined by*

$$\mathcal{C}_{n,\mathcal{T}} : pz^2 = E^2x^{12n} - G^2$$

*satisfies  $\mathcal{C}_{n,\mathcal{T}}(\mathbb{A}_{\mathbb{Q}})^{\text{Br}} = \emptyset$ .*

*Proof.* Let  $\mathfrak{C}_p$  be the set of the septuples  $(A, B, C, D, E, F, G) \in \mathbb{Z}^7$  satisfying the following two conditions:

- (i)  $(A, B, C, D, E, F, G)$  satisfies (59) and (A1), (A3), (A4), (A5), (A7) in Definition 1.1, and
- (ii) for any  $n \geq 1$ ,  $(A, B, C, D, E, F, G)$  satisfies (A6) in Definition 1.1 with respect to the couple  $(p, n)$ .

By Lemma 9.1, we know that  $\mathfrak{C}_p$  is of infinite cardinality.

Take any septuple  $\mathcal{T} := (A, B, C, D, E, F, G) \in \mathfrak{C}_p$ , and let  $\mathcal{S}_{E,G}$  be the set of odd primes  $l$  such that  $\gcd(l, 3) = \gcd(l, p) = 1$ ,  $l$  divides  $E$  and  $p$  is not a square in  $\mathbb{Q}_l^\times$ . Set

$$n_{E,G}^* := \begin{cases} \max_{l \in \mathcal{S}_{E,G}} \left( \frac{v_l(E) - v_l(G)}{6} \right) & \text{if } \mathcal{S}_{E,G} \neq \emptyset, \\ 1 & \text{if } \mathcal{S}_{E,G} = \emptyset, \end{cases}$$

and define

$$n_{E,G} := \max(1, n_{E,G}^*).$$

Let  $n$  be any integer such that  $n > n_{E,G}$ . Let  $l$  be any odd prime such that  $\gcd(l, 3) = \gcd(l, p) = 1$  and  $l$  divides  $E$ . If  $p$  is not a square in  $\mathbb{Q}_l^\times$ , then  $l$  belongs to  $\mathcal{S}_{E,G}$ . Hence, by definition of  $n_{E,G}$ , we see that

$$6n > 6n_{E,G} \geq 6n_{E,G}^* \geq v_l(E) - v_l(G),$$

which proves that the septuple  $\mathcal{T}$  satisfies (A2) with respect to  $(p, n)$ , and thus it satisfies Hypothesis FM with respect to the couple  $(p, n)$ . The last assertion follows immediately from Theorem 2.2.  $\square$

**Remark 9.4.** Let  $p$  be a prime such that  $p \equiv 1 \pmod{8}$  and  $p \equiv 2 \pmod{3}$ , and let  $n$  be a positive integer. In order to use the septuples  $(A, B, C, D, E, F, G)$  arising from Lemma 9.1 to produce generalized Mordell curves of degree  $12n$  and generalized Fermat curves of signature  $(12n, 12n, 12n)$  violating the Hasse principle explained by the Brauer-Manin obstruction following the approach described in Sections 4 and 6, we need to show that there exist infinitely many septuples  $(A, B, C, D, E, F, G)$  in Lemma 9.1 satisfying Hypothesis FM with respect to the couple  $(p, n)$ . It suffices to show that there are infinitely many septuples  $(A, B, C, D, E, F, G)$  in Lemma 9.1 satisfying (A2) with respect to  $(p, n)$ , that is,

$$v_l(E) - v_l(G) < 6n,$$

where  $l$  is any odd prime such that  $\gcd(l, 3) = \gcd(l, p) = 1$ ,  $l$  divides  $E$ , and  $p$  is not a square in  $\mathbb{Q}_l^\times$ . We will use *Schinzel's Hypothesis H* to prove that there should be infinitely many septuples  $(A, B, C, D, E, F, G)$  in Lemma 9.1 that satisfy Hypothesis FM with respect to the couple  $(p, n)$ .

We recall the statement of Schinzel's Hypothesis H (see [11]).

**Conjecture 9.5.** (*Schinzel's Hypothesis H*)

Let  $F_1(x), F_2(x), \dots, F_n(x)$  be nonconstant polynomials in  $\mathbb{Z}[x]$  such that the polynomials  $F_1(x), F_2(x), \dots, F_{n-1}(x)$  and  $F_n(x)$  have positive leading coefficients and irreducible over  $\mathbb{Q}$ . Assume that the polynomial

$$F(x) := \prod_{i=1}^n F_i(x) \in \mathbb{Z}[x]$$

has no fixed prime divisor, that is, there is no prime  $q$  dividing  $F(m)$  for all integers  $m$ . Then there are infinitely many arbitrarily large positive integers  $x$  such that  $F_1(x), F_2(x), \dots, F_{n-1}(x)$  and  $F_n(x)$  are simultaneously primes.

**Corollary 9.6.** Let  $p$  be a prime such that  $p \equiv 1 \pmod{8}$  and  $p \equiv 2 \pmod{3}$ . Let  $\mathfrak{C}_p$  be the set defined in Corollary 9.3. Assume Schinzel's Hypothesis H. Let  $n$  be a positive integer. Then there exist infinitely many septuples  $(A, B, C, D, E, F, G)$  in  $\mathfrak{C}_p$  that satisfy Hypothesis FM with respect to the couple  $(p, n)$ .

*Proof.* We maintain the same notation as in the proof of Lemma 9.1. Using exactly the same words and repeating the same arguments from the beginning of the proof of Lemma 9.1 to the end of *Step 3* in the proof of Lemma 9.1, we let  $\lambda, \gamma, \epsilon_0, \delta_0$  as in the proof of Lemma 9.1, and define  $t_0, F_0$  and  $H$  as in *Steps 1, 2* and *3* in the proof of Lemma 9.1. Let  $(A, B, C, D, E, F, G)$  be the septuple of integers defined by (59), where  $\mu$  will be determined now.

By (66), we see that

$$\begin{aligned} E &= F_0(2pF_0(\epsilon_0 + 9\mu\gamma^2) - 9\gamma^2 t_0)(2F_0(\delta_0 - p\mu\lambda^2) + \lambda^2 t_0) \\ &= F_0(2pF_0(\epsilon_0 + 9\mu\gamma^2) - 9\gamma^2(-3\lambda\gamma F_0 t_1))(2F_0(\delta_0 - p\mu\lambda^2) + \lambda^2(-3\lambda\gamma F_0 t_1)) \\ &= F_0^3(2p(\epsilon_0 + 9\mu\gamma^2) + 27\lambda\gamma^3 t_1)(2(\delta_0 - p\mu\lambda^2) - 3\lambda^3\gamma t_1) \\ &= -F_0^3((18p\gamma^2)\mu + 2p\epsilon_0 + 27\lambda\gamma^3 t_1)((2p\lambda^2)\mu - 2\delta_0 + 3\lambda^3\gamma t_1), \end{aligned}$$

and hence

$$(93) \quad E = -F_0^3 E_1^* E_2^*,$$

where

$$E_1^* := (18p\gamma^2)\mu + 2p\epsilon_0 + 27\lambda\gamma^3t_1$$

and

$$E_2^* := (2p\lambda^2)\mu - 2\delta_0 + 3\lambda^3\gamma t_1.$$

Let

$$(94) \quad \mu := 3p\mu_1,$$

where  $\mu_1$  will be determined below. We see that

$$E_1^* := (54p^2\gamma^2)\mu_1 + 2p\epsilon_0 + 27\lambda\gamma^3t_1$$

and

$$E_2^* := (6p^2\lambda^2)\mu_1 - 2\delta_0 + 3\lambda^3\gamma t_1.$$

Write  $t_1 = 2^v t_1^*$ , where  $v$  is a non-negative integer and  $t_1^*$  is an odd integer. We contend that  $t_1$  is an even integer, that is,  $v \geq 1$ . By (70), (72), (73) and since  $\lambda$  and  $\gamma$  are odd, we see that

$$1 = 27\lambda^3\gamma^3t_1 - pt_4 \equiv t_1 + t_4 \equiv t_1 + t_3 + 27\lambda^3\gamma^3t_5 \equiv t_1 + t_3 + t_5 \equiv t_1 + 1 \pmod{2},$$

and hence

$$t_1 \equiv 0 \pmod{2}.$$

Thus  $t_1$  is an even integer, and therefore  $v \geq 1$ .

We see that

$$(95) \quad E_1^* = 2E_1$$

and

$$(96) \quad E_2^* = 2E_2,$$

where

$$(97) \quad E_1 := (27p^2\gamma^2)\mu_1 + p\epsilon_0 + 27\lambda\gamma^32^{v-1}t_1^*$$

and

$$(98) \quad E_2 := (3p^2\lambda^2)\mu_1 - \delta_0 + 3\lambda^3\gamma2^{v-1}t_1^*.$$

Let  $Q_1^*$  be the integer defined by (79) in *Step 4* in the proof of Lemma 9.1. We can write  $Q_1^*$  in the form

$$(99) \quad Q_1^* = P_2^*\mu + R_2^* = 3pP_2^*\mu_1 + R_2^*,$$

where we recall from *Step 4* in the proof of Lemma 9.1 that

$$P_2^* = 18\lambda^2\gamma^2$$

and

$$R_2^* = 2\lambda^2\epsilon_0 + t_4.$$

Viewing  $\mu_1$  as a variable, we see that  $E_1, E_2$  and  $Q_1^*$  are polynomials with integral coefficients in the variable  $\mu_1$ , i.e.,  $E_1, E_2$  and  $Q_1^*$  belong to  $\mathbb{Z}[\mu_1]$ . Upon assuming Schinzel's Hypothesis H, we will show that there should be infinitely many arbitrarily large positive integers  $\mu_1$  such that  $E_1, E_2$  and  $Q_1^*$  are simultaneously primes. In order to apply Schinzel's Hypothesis H, we need to prove that the polynomial  $\Psi(\mu_1) \in \mathbb{Z}[\mu_1]$  defined by

$$(100) \quad \Psi(\mu_1) := E_1 E_2 Q_1^*$$

has no fixed divisors, that is, there is no prime  $q$  dividing  $\Psi(m)$  for every integer  $m$ . To prove the latter, it suffices to show that

$$\gcd(27p^2\gamma^2, p\epsilon_0 + 27\lambda\gamma^32^{v-1}t_1^*) = 1,$$

$$\gcd(3p^2\lambda^2, -\delta_0 + 3\lambda^3\gamma 2^{v-1}t_1^*) = 1,$$

and

$$\gcd(3pP_2^*, R_2^*) = 1.$$

Using the same arguments as in *Step 4* in the proof of Lemma 9.1, we see that

$$(101) \quad \gcd(3pP_2^*, R_2^*) = 1.$$

We now prove that

$$\gcd(27p^2\gamma^2, p\epsilon_0 + 27\lambda\gamma^3 2^{v-1}t_1^*) = 1.$$

Indeed, by (73), we see that

$$2^{v-1}t_1^* = \frac{t_1}{2} \equiv \frac{1}{54\lambda^3\gamma^3} \not\equiv 0 \pmod{p}.$$

Since  $\gcd(p, \lambda) = \gcd(p, \gamma) = \gcd(p, 3) = 1$ , we deduce that

$$p\epsilon_0 + 27\lambda\gamma^3 2^{v-1}t_1^* \equiv 27\lambda\gamma^3 2^{v-1}t_1^* \not\equiv 0 \pmod{p}.$$

Since  $\gcd(\lambda, 3\gamma) = 1$ , we see that if  $l$  is any prime dividing  $3\gamma$ , then it follows from (62) that

$$p\epsilon_0 \equiv \frac{1}{\lambda^2} \not\equiv 0 \pmod{l},$$

and hence

$$p\epsilon_0 + 27\lambda\gamma^3 2^{v-1}t_1^* \equiv p\epsilon_0 \not\equiv 0 \pmod{l}.$$

Thus we deduce that

$$(102) \quad \gcd(27p^2\gamma^2, p\epsilon_0 + 27\lambda\gamma^3 2^{v-1}t_1^*) = 1.$$

We prove that

$$\gcd(3p^2\lambda^2, -\delta_0 + 3\lambda^3\gamma 2^{v-1}t_1^*) = 1.$$

Indeed, by (62) and (73), we see that

$$\begin{aligned} -\delta_0 + 3\lambda^3\gamma 2^{v-1}t_1^* &= -\delta_0 + 3\lambda^3\gamma \left(\frac{t_1}{2}\right) \equiv -\frac{1}{9\gamma^2} + 3\lambda^3\gamma \left(\frac{1}{54\lambda^3\gamma^3}\right) \\ &\equiv -\frac{1}{9\gamma^2} + \frac{1}{18\gamma^2} \\ &\equiv -\frac{1}{18\gamma^2} \not\equiv 0 \pmod{p}. \end{aligned}$$

By (63), we see that

$$-\delta_0 + 3\lambda^3\gamma 2^{v-1}t_1^* \equiv -\delta_0 \equiv -2 \equiv 1 \pmod{3}.$$

By (62) and since  $\gcd(\lambda, 3\gamma) = 1$ , we see that if  $l$  is any prime dividing  $\lambda$ , then

$$-\delta_0 + 3\lambda^3\gamma 2^{v-1}t_1^* \equiv -\delta_0 \equiv -\frac{1}{9\gamma^2} \not\equiv 0 \pmod{l}.$$

Therefore we deduce that

$$(103) \quad \gcd(3p^2\lambda^2, -\delta_0 + 3\lambda^3\gamma 2^{v-1}t_1^*) = 1.$$

By (101), (102), (103), we see that the polynomial  $\Psi$  defined by (100) has no fixed prime divisor. On the other hand,  $E_1, E_2$  and  $Q_1^*$  have positive leading coefficients and irreducible over  $\mathbb{Q}$ . Hence Schinzel's Hypothesis H expects that there should be infinitely many arbitrarily large positive integers  $\mu_1$  such that  $E_1, E_2$  and  $Q_1^*$  are simultaneously primes. Take such a positive integer  $\mu_1$ , and define  $\mu$  by (94). We see that the choice of  $\mu$  here is *compatible* with that of  $\mu$  in *Step 4* in the proof of Lemma 9.1. More precisely, in *Step 4* in the proof of Lemma 9.1, we chose  $\mu$  so that  $\mu = 3p\mu_1$  and  $Q_1^* = 3pP_2^*\mu_1 + R_2^*$  is an odd prime for some integer  $\mu_1$ , and it is not difficult to realize that the choice of  $\mu$  here satisfies these conditions. Repeating the same arguments as in *Steps 5, 6, 7, 8* and *9* in the proof of Lemma 9.1, we



deduce that the septuple  $(A, B, C, D, E, F, G)$  satisfies (A1) and (A3) – (A7) with respect to the couple  $(p, n)$ . It remains to prove that  $(A, B, C, D, E, F, G)$  satisfies (A2) with respect to the couple  $(p, n)$ .

By (93), (95) and (96), we see that

$$E = -4F_0^3 E_1 E_2.$$

Let  $l$  be any odd prime such that  $\gcd(l, 3) = \gcd(l, p) = 1$  and  $l$  divides  $E$ . Then either  $l$  divides  $F_0$  or  $\gcd(l, F_0) = 1$  and  $l$  divides  $E_1 E_2$ . If  $l$  divides  $F_0$ , then it follows from (F1) and (F2) in *Step 3* in the proof of Lemma 9.1 that  $p$  is a square in  $\mathbb{Q}_l^\times$ . If  $l$  does not divide  $F_0$  and  $l$  divides  $E_1 E_2$ , then since  $E_1, E_2$  are odd primes, it follows that

$$v_l(E) = v_l(-4F_0^3 E_1 E_2) = v_l(E_1 E_2) \leq 2.$$

Thus we deduce that

$$v_l(E) - v_l(G) \leq 2 + 0 = 2 < 6n.$$

Thus  $(A, B, C, D, E, F, G)$  satisfies (A2) with respect to the couple  $(p, n)$ . Since  $(A, B, C, D, E, F, G)$  is defined by (59), it follows that  $(A, B, C, D, E, F, G)$  belongs to  $\mathfrak{C}_p$  and satisfies Hypothesis FM with respect to the couple  $(p, n)$ . Hence our contention follows.  $\square$

#### ACKNOWLEDGEMENTS

I would like to thank Mike Bennett and Bjorn Poonen for their comments. I thank Dinesh Thakur for his interest in this work. I am grateful to Romyar Sharifi for funding me under his NSF Grant DMS-0901526 in the fall of 2011 when part of this work was written. I was supported by a postdoctoral fellowship in the Department of Mathematics at University of British Columbia.

#### REFERENCES

- [1] M.A. BENNETT AND C.M. SKINNER, *Ternary Diophantine equations via Galois representations and modular forms*, Canad. J. Math. **56** (2004), no. 1, pp. 23–54.
- [2] H. COHEN, *Number Theory, Volume I: Tools and Diophantine equations*, Graduate Texts in Math. **239**, Springer-Verlag (2007).
- [3] D. CORAY AND C. MANOIL, *On large Picard groups and the Hasse principle for curves and K3 surfaces*, Acta. Arith. **76** (1996), pp. 165–189.
- [4] E. HALBERSTADT AND A. KRAUS, *Courbes de Fermat: résultats et problèmes*, J. Reine Angew. Math **548** (2002), pp. 167–234.
- [5] W. IVORRA AND A. KRAUS, *Quelques résultats sur les équations  $ax^p + by^p = cz^2$* , Canad. J. Math. **58** (2006), no. 1, pp. 115–153.
- [6] C.E. LIND, *Untersuchungen über die rationalen Punkte der ebenen kubischen Kurven vom Geschlecht Eins*, Thesis, University of Uppsala (1940).
- [7] YU.I. MANIN, *Le groupe de Brauer-Grothendieck en géométrie Diophantienne*, Actes du Congrès International des Mathématiciens, Nice (1970), pp. 401–411.
- [8] B. POONEN, *Rational points on varieties*, Available at <http://www-math.mit.edu/~poonen/papers/Qpoints.pdf>, (2008).
- [9] H. REICHARDT, *Einige im Kleinen überall lösbar, im Grossen unlösbar diophantische Gleichungen*, J. Reine Angew. Math. **184** (1942), pp. 12–18.
- [10] A. SCHINZEL, *Remarks on the paper “Sur certaines hypothèses concernant les nombres premiers”*, Acta. Arith. **7** (1961/1962), 1–8.
- [11] A. SCHINZEL AND W. SIERPIŃSKI, *Sur certaines hypothèses concernant les nombres premiers*, Acta. Arith. **4** (1958), 185–208; corrigé ibid. **5** (1958).
- [12] E.S. SELMER, *The Diophantine equation  $ax^3 + by^3 + cz^3 = 0$* , Acta. Math. **85** (1951), pp. 203–362.
- [13] A.N. SKOROBOGATOV, *Torsors and rational points*, CTM **144**. Cambridge Univ. Press (2001).
- [14] A. WILES, *Modular elliptic curves and Fermat’s last theorem*, Ann. of Math. (2) **141** (1995), no.3, 443–551.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF BRITISH COLUMBIA, VANCOUVER, BRITISH COLUMBIA, V6T 1Z2, CANADA

*E-mail address:* dongquan@math.ubc.ca, dongquan.nndq@gmail.com